Description of document:	Naval Criminal Investigative Service (NCIS) manuals 1 and 2, and NCIS Service Managers Internal Control (MIC) Plan, 2007-2016
Requested date:	14-December-2015
Released date:	04-April-2016
Posted date:	23-May-2016
Source of document:	Naval Criminal Investigative Service Headquarters (Code 00LJF) 27130 Telegraph Road Quantico, VA 22134-2253 E-mail: ncis_foia@ncis.navy.mil Fax: (571) 305-9867

DEPARTMENT OF THE NAVY
HEADQUARTERS
NAVAL CRIMINAL INVESTIGATIVE SERVICE
27130 TELEGRAPH ROAD
QUANTICO VA 22134-2253

5720 2016-002026
SER00LJF/16U0476

APR 04 2016

This further responds to your December 14, 2015 Freedom of Information Act (FOIA) request seeking Naval Criminal Investigative Service (NCIS) manuals 1, 2 and 3 and the NCIS Service Managers Internal Control (MIC) Plan. Your request was received in this office on December 14, 2015.

To accommodate you, we composed this partial release. The processing of the first two manuals and the MIC Plan has been completed. Our review of the documents reveals that they contain personal identifiers (such as names and emails) of third parties, the release of which would constitute an unwarranted invasion of personnel privacy. Accordingly, we must partially deny your request and withhold this information pursuant to the FOIA 5 U.S.C. § 552(b)(6). Exemptions (b)(7)(D) and (b)(7)(E) have also been cited. We have also provided an enclosure explaining the various exemptions of the FOIA.

If you would like to appeal any adverse determination, I am advising you of your right to appeal. Your appeal must be postmarked within 60 calendar days from the date of this letter and should be addressed to the Secretary of the Navy's designee: Office of the Judge Advocate General, (Code 14), 1322 Patterson Avenue, S.E., Suite 300, Washington Navy Yard, D.C. 20374-5066. The envelope and letter should bear the annotation "FOIA Appeal." Please include a copy of your original request with your appeal letter.

There are no assessable fees associated with the processing of your request. Once the processing of the remaining manual has been completed, we will further correspond with you. If you have any questions regarding this matter, please contact our office at (571) 305-9092 or via email at ncis_foia@ncis.navy.mil.

Sincerely,

KAREN RICHMAN
CDR(S), JAGC, USN

Encl:
(1) CD/Documents

NCIS

Explanation of FOIA/PA Exemptions

Subsections of Title 5, United States Code, Section 552

(b)(1) (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified to such Executive order;

(b)(2) related solely to the internal personnel rules and practices of an agency;

(b)(3) specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute(A) requires that the matters be withheld from the public in such a manner as to leave no discretion on issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;

(b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(b)(6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy;

(b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could be reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could be reasonably expected to constitute an unwarranted invasion of personal privacy, (D) could reasonably be expected to disclose the identity of confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual;

(b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or

(b)(9) geological and geophysical information and data, including maps, concerning wells.

Subsections of Title 15, United States Code, Section 552a

(d)(5) information compiled in reasonable anticipation of a civil action proceeding;

(j)(2) material reporting investigative efforts pertaining to the enforcement of criminal law including efforts to prevent, control, or reduce crime or apprehend criminals;

(k)(1) information which is currently and properly classified pursuant to an Executive order in the interest of the national defense or foreign policy, for example, information involving intelligence sources or methods;

(k)(2) investigatory material compiled for law enforcement purposes, other than criminal, which did not result in loss of a right, benefit or privilege under Federal programs, or which would identify a source who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(3) material maintained in connection with providing protective services to the President of the United States or any other individual pursuant to the authority of Title 18, United States Code, Section 3056;

(k)(4) required by statute to be maintained and used solely as statistical records;

(k)(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment or for access to classified information, the disclosure of which would reveal the identity of the person who furnished information pursuant to a promise that his/her identity would be held in confidence;

(k)(6) testing or examination material used to determine individual qualifications for appointment or promotion in Federal Government service the release of which would compromise the testing or examination process;

(k)(7) material used to determine potential for promotion in the armed services, the disclosure of which would reveal the identity of the person who furnished the material pursuant to a promise that his/her identity would be held in confidence.

NCIS 1, CHAPTER 1
NAVAL CRIMINAL INVESTIGATIVE SERVICE HISTORY
EFFECTIVE DATE: AUGUST 2013

Table of Contents

Reference:
(a) SECNAVINST 5430.107 dated December 28, 2005

1-1. Purpose. This chapter establishes the history and background of the Naval Criminal Investigative Service (NCIS) from its early conception to being one of the premier Federal law enforcement agencies of the 21st Century. During its dynamic history, NCIS has been known by different names but it has always been an agency that leads in responding to the revolving challenges of the criminal, counterintelligence and security community.

1-2. Policy. None.

1-3. Cancellation. NCIS-1, Chapter 3, Naval Criminal Investigative History, January 2008.

1-4. Chapter Sponsor. The chapter sponsor for this chapter is NCIS Communications, Code 00C.

1-5. History

a. The origins of the Naval Criminal Investigative Service (NCIS) date from a Navy "General Plan" prepared in 1915, which assigned to Naval Intelligence the task of securing information on the navies of probable enemies. The plan contemplated obtaining information by both overt and covert means, and, in the fall of 1916, the first branch office (a small undercover unit) was established in New York City under the supervision of the Office of Naval Intelligence (ONI). Heavy reliance was placed on reserve, active duty, and civilian operatives, many of the latter serving voluntarily and without pay. The office served as a model for others developed

during World War I and accounted for some impressive successes in the field of counterespionage.

b. This early entry into internal security extended to criminal investigations. Responsibility for investigative activities was placed under Naval Aides for Information, who were locally assigned to the staffs of each of the 15 Naval District Commandants. Later, all investigative activities were placed under the District Aide.

c. Rapid demobilization and the desire for a return to normalcy after World War I saw investigative activity reduced to a virtual standstill. The District Aide evolved into the District Intelligence Officer, usually a one-person office. This intelligence officer, through the use of paid confidential informants, handled investigative requirements that arose. In early 1926, initiatives were undertaken to organize special groups of volunteer reserve intelligence officers who were envisioned as a means of obtaining information on persons and activities that might constitute a threat to the naval establishment, as well as providing a cadre of trained personnel in the event of national emergency. By March 1927, these units had been organized, and their operations were refined in succeeding years through the early 1930s.

d. During the early and mid-1930's the development of an independent professional investigative capability within the Navy was being nurtured. Efforts to enroll more reserve officers in the inactive Intelligence Reserve were making progress. In Washington, D.C., the first civilian agent was employed in 1936 on a verbal basis and paid by personal check of the Director of Naval Intelligence. He was followed by a small handful of civilian special agents who were seeded throughout the districts beginning in 1936, although by September of 1937 they numbered only 14 nationwide. Operating independently and with little guidance, these individuals proved remarkably resourceful and effective, and formed the genesis of our modern professional agent corps.

e. In June 1939, President Roosevelt directed that ONI handle the investigation of Navy cases relating to sabotage, espionage and subversive activities, and an agreement delineating these responsibilities among interested Federal agencies was entered into the following year. By the fall of 1940, selective call-up of intelligence reservists for investigative and counterintelligence duties was undertaken on a broad scale, and following entry into World War II, the Navy's investigative arm was manned almost exclusively by reserve officers. Their primary tasks related to personnel security inquiries, sabotage and espionage cases, investigation of Japanese activities in the United States, and war fraud matters. A peak was reached in 1943 when over 97,000 separate investigations were conducted by what was known as the "Naval Intelligence Service."

f. At the conclusion of World War II, there was again a general demobilization, resulting in only a small corps of civilian special agents being retained. Although the Secretary of the Navy extended investigative jurisdiction in 1945, no meaningful expansion of personnel occurred until the Korean conflict, when a major buildup of civilian agents took place.

1-6. Naval Investigative Service

a. Until the late 1950s, District Intelligence Office operations were under the command supervision of Naval District Commandants, and investigative effort was frequently parochial, fragmented, and on occasion, duplicative from one district to another. Workload, manpower, and jurisdiction in investigations and counterintelligence broadened following the Korean conflict. A number of significant changes in organization and policy occurred during the 1950s and 1960s, as well as refinements in mission, which culminated in the establishment of the Naval Investigative Service (NIS) in February 1966. From this date forward, the NCIS mission has been primarily criminal investigative and counterintelligence support to the Department of the Navy (DON).

b. In October 1972, personnel security investigative responsibilities and functions were transferred from NIS to the newly created Defense Investigative Service (DIS). One half of NIS' special agents were transferred to the newly established DIS in order for it to immediately begin to fulfill its mission.

c. In October 1981, NIS became a Second Echelon Command under the Chief of Naval Operations. In August 1985, the Secretary of the Navy directed the appointment of a flag rank naval officer to hold the position of Commander, NIS, reporting directly to the Chief of Naval Operations and the Secretary of the Navy. Rear Admiral Cathal Flynn was assigned as the first flag officer to command NIS.

1-7. Naval Security and Investigative Command

a. On November 15, 1985, NIS was re-designated as the Naval Security and Investigative Command (NSIC) and broadened its missions to include management of the DON Security Program. These programs included naval information, physical, and personnel security; adjudication for security clearances; and Navy law enforcement and physical security. This resulted in NSIC also assuming control of the Navy's Master-at-Arms program and the military working dog program. The Navy's Anti-Terrorist Alert Center was also established during this timeframe.

b. In 1986, NSIC opened the DON's Central Adjudication Facility (DONCAF) to review security clearance investigations conducted by DIS to determine suitability for the issuance or retention of security clearances. DONCAF adjudicated security clearances for the Navy, the Marine Corps, and for all civilians working within the DON.

(1) On September 27, 1988, NSIC was changed to the Naval Investigative Service Command (NISC).

(2) In December 1993, the Secretary of the Navy abolished the position of the flag rank officer as Commander of NISC, and established a civilian Director, a Senior Executive Service (SES) position. At the same time, NISC was renamed as the Naval Criminal Investigative Service (NCIS), and was aligned as an echelon two activity under the Secretary of the Navy, via the General Counsel. The Secretary of the Navy appointed Roy D. Nedrow, former U.S. Secret Service Deputy Assistant Director, as the first civilian Director of NCIS.

1-8. Naval Criminal Investigative Service

a. In September 1995, NCIS established the Cold Case Homicide Unit. NCIS was the first Federal law enforcement agency to fully dedicate a department to cold case investigations, and, as of January 2013, the unit had resolved 63 homicides.

b. In May 1997, Secretary of the Navy John Dalton appointed Special Agent David L. Brant as the second civilian Director of NCIS.

c. In 1999, NCIS and the Marine Corps Criminal Investigation Division (CID) signed a memorandum of understanding integrating Marine Corps CID investigators into NCIS for the investigation of criminal offenses and other matters.

d. In November 2000, the United States Congress passed legislation authorizing the Secretary of the Navy to grant NCIS civilian special agents authority to execute Federal warrants and make arrests of civilians.

e. In October 2000, the Navy warship USS Cole (DDG-67) was attacked in Aden, Yemen by terrorists, resulting in the deaths of 17 United States Navy Sailors. NCIS and Federal Bureau of Investigation agents immediately began an investigation which lasted for several months. Their efforts resulted in the indictment and conviction of several terrorists.

f. In January 2002, NCIS transformed the Antiterrorist Alert Center (ATAC) into the Multiple Threat Alert Center (MTAC) as a result of the growing appreciation of the changing threats facing the DON.

g. In 2003, NCIS established the Law Enforcement Information Exchange (LInX) in the Pacific Northwest and Hampton Roads, Virginia. LInX is an information sharing initiative which provides participating law enforcement personnel the ability to electronically search and review the law enforcement records of all other participating agencies in a particular region. Other regions, including Hawaii, New Mexico, South Texas, Southeast Georgia/Northeast Florida, the National Capital Region of Washington, DC, North Carolina, Southern California and the Northeast have since been added. In 2008, NCIS created the Department of Defense Law Enforcement Exchange (D-DEx), which is connected to LInX and shares law enforcement data among the military criminal investigative organizations and other DoD law enforcement agencies.

h. In September 2003, NCIS deployed its first agents to Iraq to conduct protective service operations and provide counterterrorism, counterintelligence, and criminal investigative support.

i. On December 28, 2005, the Secretary of the Navy issued the reference which establishes the NCIS charter, updating the responsibilities, mission and functions of NCIS and its relationships with other DON organizations and activities.

j. In January 2006, Special Agent Thomas A. Betro was appointed the third civilian Director of the NCIS by Secretary of the Navy, Donald C. Winter.

k. In February 2010, Special Agent Mark D. Clookie was sworn in as the fourth civilian Director of NCIS by Secretary of the Navy, Ray Mabus.

l. In June 2010, NCIS undertook a reorganization to enhance mission focus and improve both the efficiency and the effectiveness of the organization. Key changes effected by the reorganization, which was approved by the Under Secretary of the Navy, include the creation of a single Deputy Director position, the combination of the existing Combating Terrorism and Counterintelligence Directorates (Codes 21 and 22) into a single directorate (renamed the National Security Directorate) and the creation of a Global Operations Directorate. The Global Operations Directorate was established to direct field elements in a number of major functional areas that had in recent years been directed from NCIS Headquarters.

m. In October 2012, after a review of the security functions within DON, the Deputy Under Secretary of the Navy for Plans, Policy, Oversight, and Integration (DUSN (PPOI)) was

designated as the DON Security Executive. The Director of NCIS retains responsibility for Naval investigative matters, but no longer continues as the CNO Special Assistant for Naval Security.

n. In January 2013, the DONCAF was consolidated, along with the other Central Adjudications Facilities within DoD, into a single organization, known as the DoD CAF, per the direction of the Deputy Secretary of Defense.

o. As of March 2013, NCIS operates from 19 field offices, including five functional field offices, and more than 150 individual locations around the globe, including every aircraft carrier and "big-deck" amphibious assault vessel.

p. Through the accomplishment of its diverse criminal, counterintelligence, and security mission, NCIS continues to provide critical worldwide service to the DON, its military and civilian personnel, their dependents and the communities in which they reside.

NCIS-1, CHAPTER 2
Naval Criminal Investigative Service Mission, Organizational Structure, Roles, and Responsibilities of the Executive Staff
September 2013

2-1. Purpose. To set forth policy, organizational mission and functions, and organizational hierarchy and responsibilities of executive leadership and senior managers by:

a. Identifying the Naval Criminal Investigative (NCIS) mission, organizational flow, and hierarchy.

b. Establishing the roles and responsibilities of the program and field operational executive staff, senior headquarters management, and special agents in charge.

c. Establishing the lines of accountability for the Director; Deputy Director; Principal Executive Assistant Director for Management and Administration; Executive Assistant

Directors (Criminal Investigations, National Security, Atlantic and Pacific Operations, and Global Operations); Chiefs of the support directorates (Intelligence and Information Sharing; Financial Management and Planning; and Information Technology); Assistant Directors; Deputy Assistant Directors; Special Agents in Charge; and the Director's immediate staff.

d. Defining management and leadership terminology describing functions, authorities, and responsibilities.

2-2. Policy

a. SECNAVINST 5430.107 of December 28, 2005, sets forth the authority, responsibilities, mission, and functions of NCIS and its relationship with other Department of the Navy (DON) organizations and activities. This instruction is available on Lighthouse, NCIS' intranet, and the DON Issuances website (http://doni.daps.dla.mil/default.aspx).

b. NCIS exists to preserve U.S. Navy and U.S. Marine Corps' operational readiness as well as prevent current and future warfighting capabilities from being degraded by terrorism, foreign intelligence activities, or criminal activity. NCIS' ability to collect, process, and provide timely, high-quality and actionable information to the senior leaders of the DON and its military commanders, through investigations, operations, and source networks, ensures NCIS remains a critically relevant and essential element of the DON's continued success.

c. The Director, NCIS reports directly to the Secretary of the Navy. The Under Secretary of the Navy, with the assistance of the General Counsel of the Navy, has oversight of NCIS and serves as chair of the NCIS Board of Directors. The Director, NCIS is authorized to organize, assign, and reassign responsibilities among NCIS subordinate activities.

2-3. Cancellation. NCIS-1, Chapter 2–NCIS Mission and Organizational Structure of June 2007 and NCIS Policy Document 10-16: Administrative (NCIS Organizational Codes and Titles) Gen Admin 11C-0033 released November 16, 2010.

2-4. Chapter Sponsor. The chapter sponsor is the Administrative Services Department, Code 11C.

2-5. Physical Infrastructure. NCIS Headquarters is located in the Russell-Knox Building in Quantico, Virginia. NCIS maintains a worldwide presence with 19 field offices and more than 150 other locations around the globe.

2-6. Mission and Organizational Hierarchy. Operational authority in NCIS flows from the Director through the Deputy Director. A staff of executive officers, advisers, and assistants report directly to the Director.

a. Mission. NCIS is a federal law enforcement agency that protects and defends the DON against terrorism and foreign intelligence threats, investigates major criminal offenses, enforces the criminal laws of the United States and the Uniform Code of Military Justice, assists commands in maintaining good order and discipline, and provides law enforcement and security

services to the U.S. Navy and U.S. Marine Corps worldwide. The NCIS is centrally managed and resourced from Headquarters; the operational mission is executed in a decentralized manner by field offices, resident agencies, and resident units. Responsibilities of the Director, Deputy Director, Director's staff, as well as NCIS Headquarters and field directorates are detailed in section 2-8 through 2-28.

b. Organizational Hierarchy. NCIS Headquarters is an Echelon 2 activity within the DON and is led by a Director (Senior Executive Service federal government employee). The Director has a staff of senior executives and senior managers who report to him/her through an established organizational hierarchy.

(1) Director.

(2) Executive Staff.

(a) Deputy Director.

(b) Principal Executive Assistant Director, Management & Administration.

(c) Executive Assistant Director, Criminal Investigations.

(d) Executive Assistant Director, National Security.

(e) Executive Assistant Director, Pacific Operations.

(f) Executive Assistant Director, Atlantic Operations.

(g) Executive Assistant Director, Global Operations.

(h) Chief, Intelligence and Information Sharing.

(i) Chief, Financial Management and Planning.

(3) Senior Managers.

(a) Assistant Director, Human Resources.

(b) Assistant Director, Administration and Logistics .

(c) Assistant Director, Criminal Investigations.

(d) Assistant Director, National Security.

(e) Assistant Director, Information Technology.

(f) Deputy Assistant Directors .

(g) Special Agent in Charges.

(4) Director's Staff.

(a) Communications Director.

(b) Inspector General.

(c) Counsel.

(d) Chief Diversity Manager/Deputy Equal Employment Officer.

(e) Chief of Staff .

(f) Comptroller.

(3) Operational Hierarchy – Headquarters. Organizational support required to meet directorate-level mission requirements is accomplished through Programs.

(4) Operational Hierarchy – Field Offices. Each field office Special Agent in Charge maintains organizational responsibility for subordinate Field Office investigative/operational squads, NCIS resident agencies (NCISRAs), and NCIS resident units (NCISRUs). Squads and NCISRAs are subordinate to a field office and are managed by a Supervisory Special Agent. NCISRUs are operationally and administratively subordinate to and supported by a NCISRA, commonly called the "parent NCISRA." NCISRUs are staffed by at least one Special Agent. In NCISRUs with more than one Special Agent, the SAC may designate a Senior Resident Agent and delegate authority for specified operational and/or administrative matters.

2-7. Key Management and Leadership Terms. The following terms describe the functions, authorities, and responsibilities for each executive or senior manager. These words were carefully chosen to help clarify roles and responsibilities, and to increase accountability for operational and administrative activity.

a. Accountable. To be answerable for an action or result, or for carrying out a function.

b. Advise and Inform. To notify or assist others in understanding a function, activity, product, process, or concept to a degree that others can prepare, produce, conduct, and act in an appropriate, accurate, and sufficient manner.

c. Collaborate and Participate. To work with others and contribute substantially without having the sole responsible to produce specific products or actions.

d. Coordinate and Facilitate. To assist others in enabling a desired outcome without being responsible for specific products or actions.

e. Direct. To be in command of and accountable for the outcome produced by those who actually conduct an action or series of actions.

f. Ensure. To be responsible for seeing that a product or action is completed, without being responsible for the specific function.

g. Impact. To cause something to happen that would not have happened without the occurrence of an intentional action.

h. Lead. To establish direction and influence others to follow that direction.

i. Manage. To be in charge of and responsible for the completion of an action or series of actions and their outcomes through the supervision of others.

j. Oversee. To supervise others who are responsible for the completion of an action or a series of actions and the outcome.

k. Prepare and Produce. To take action and be accountable for accuracy, consistency, sufficiency, and outcome.

l. Provide/Submit. To give requested information, data, projections or estimates to those who have responsibility for a function.

m. Responsible. To be obligated to produce an action or outcome in such a manner that a person may be blamed or credited.

n. Review. To provide substantive input on the accuracy, consistency, and sufficiency of the product or action of another.

o. Supervision. A management activity; the responsibility for a subordinate's progress, productivity, and evaluation.

2-8. Director

a. NCIS Chief Executive Officer.

b. Directs the activities of the NCIS; maintains responsibility for the performance of NCIS and all activities in which it engages. The Director exercises leadership through a strategic vision and exercises its direction through the Deputy Director.

c. Maintains accountability to the Secretary of the Navy for successfully achieving the NCIS investigative and operational missions and effectively managing its administrative activities.

(1) Is directly supervised by the Under Secretary of the Navy with the assistance of the General Counsel of the Navy.

(2) Is guided by the NCIS Board of Directors, an advisory group chaired by the Under Secretary of the Navy that includes the General Counsel of the Navy, Vice Chief of Naval Operations, Assistant Commandant of the Marine Corps, and NCIS Director.

d. Roles and Responsibilities of the Director

(1) Provides leadership for the NCIS.

(a) Initiates strategic planning efforts.

(b) Publishes planning guidance and focus annually in the "Fiscal Year Focus Annex," a supplement to the NCIS Strategic (Five-Year) Plan.

(c) Establishes and communicates the agency's strategic vision, direction, and priorities.

(d) Is informed by advice and counsel of the NCIS Board of Directors, Secretary of the Navy, Chief of Naval Operations, and Commandant of the Marine Corps. Annual guidance documents informs the following NCIS strategic planning documents:

1. The NCIS Strategic Plan.

2. Program Direction Documents.

3. Regional Performance Plans.

4. Field Office Tactical Plans.

(2) Approves the NCIS Strategic Plan.

(a) Oversees the activities of the NCIS which is executed through his/her direction to, and management of, the Deputy Director and his/her supervision of the Director's immediate staff.

(b) Engages executive-level communications, internally and externally, in order to advise and inform NCIS employees and stakeholders.

1. Articulates NCIS policy positions and equities.

2. Educates and influence stakeholders and liaison partners.

3. Shares information of value.

2-9. Deputy Director

a. Serves as the NCIS Chief Operating Officer.

b. Responsible for the day-to-day oversight and management of the NCIS and its activities including the two operational directorates (Criminal Investigations and National Security), the operational support directorate (Intelligence and Information Sharing), the three field directorates, and the Management and Administration Directorate.

c. Accountable to the Director for NCIS' success in achieving its investigative and operational mission and the effective management of its administrative activities.

d. Establishes NCIS priorities and performance requirements and directs the strategic planning process for the programs.

(1) Guided by the Director's vision as articulated in the Director's Strategic Vision and his guidance focus that is published annually and through daily interactions.

(2) Produces the NCIS strategic planning documents for the Director's review and ultimate approval.

e. Roles and Responsibilities of the Deputy Director

(1) Acts in the Director's absence.

(2) Executes Director-delegated authorities and powers.

(3) Directs the NCIS strategic planning and policy development processes. Tasks the executive assistant directors with strategic planning and policy development activities and requirements.

(a) Reviews program planning and policy and policy position drafts for accuracy, relevance, and consistency with senior guidance and agency priorities.

(b) Produces final strategic planning products for Director's approval.

1. NCIS Strategic Plan.

2. Program Direction Documents.

3. Field Office Tactical Plans.

(c) Produces final policy and policy position products for Director's approval.

(d) Serves as the primary decision maker for planning and policy development processes.

(4) Oversees and manages the day-to-day activities of the executives responsible for the NCIS directorates.

(a) Executes through direction to, and supervision of, the Executive Assistant Directors.

(b) Reviews and evaluates Executive Assistant Director performance.

(5) Engages executive-level communications, internally and externally, to advise and inform NCIS employees and stakeholders:

(a) Keeps the Director informed on all major policy and operational matters.

(b) Articulates NCIS and Director's policy positions and equities.

(c) Educates and influences stakeholders and liaison partners.

(d) Shares information of value.

(6) Supervises the Chief of Staff; manages the Deputy's Staff through direction to, and supervision of, the Chief of Staff.

2-10. Principal Executive Assistant Director for Management & Administration

a. Serves as the NCIS Chief Management Officer.

b. Responsible for the day-to-day oversight and management of business operations ("end-to-end" financial, logistic, facility management, human capital, acquisition, administrative, and other functions that support the operational mission), including the activities of two administrative directorates (Human Resources and Administration & Logistics) and the Information Technology and Fiscal Management and Planning Offices; enables optimal operational performance by ensuring NCIS management and administration collaboration with the strategic planning, programming, and resourcing efforts of the operations directorates.

c. Accountable to the Deputy Director for the effective management of administrative activities and to ensure that business operations are optimally integrated to achieve operational success.

d. Manages the strategic planning process through oversight of the management and administration's planning apparatus.

(1) Responds to the Director's Strategic Vision and the priorities and performance requirements established by the Deputy Director.

(2) Provides strategic planning documents for the Deputy Director's review, concurrence, and presentation to the Director for ultimate approval.

e. Roles and Responsibilities of the Principal Executive Assistant Director

(1) When directed, acts in the Deputy Director's absence.

(2) Executes Director- and Deputy Director-delegated authorities and powers.

(3) Manages the strategic planning process.

(a) Tasks the Chief, Fiscal Management and Planning to collaborate with the Executive Assistant Directors, Chiefs, and Assistant Directors on the development of strategic planning activities and requirements and prepare draft strategic planning documents.

(b) Reviews strategic planning documents for accuracy, relevance, and consistency with senior guidance and agency priorities.

(c) Produces draft strategic planning documents for Deputy Director review.

(4) Oversees the policy development process.

(a) Tasks the Assistant Director, Administration & Logistics to collaborate with the Executive Assistant Directors, Chiefs, and Assistant Directors on agency policy development activities and requirements.

(b) Reviews and ensures policy and policy position drafts are accurate, relevant, and consistent with senior guidance and NCIS and DON priorities.

(c) Produces final policy and policy position products for Deputy Director review and concurrence, and presentation to the Director for review and approval.

(5) Oversees the activities of the Management & Administrative Directorate. Informed by the Deputy Director's priorities and performance requirement; executes through direction to, and supervision of, the Assistant Directors and Chiefs.

(a) Reviews and evaluates Chief and Assistant Director's performances.

(b) Consults with the Director and Deputy Director on key program, administration, and personnel decisions.

(6) Engages executive-level communications, internally and externally, in order to advise and inform employees and stakeholders.

(a) Keeps the Director and Deputy Director informed on all major policy and management and administrative matters.

(b) Articulates policy positions and equities of NCIS and Director and Deputy Director.

(c) Educates and influences stakeholders, resource sponsors, and liaison partners. Serve as the primary NCIS point of contact for matters under Management & Administrative Directorate purview.

(d) Shares information of value.

2-11. Executive Assistant Director for Criminal Investigations

a. Serves as the Chief Executive Officer for the NCIS Criminal Investigations Directorate.

b. Directs the activities conducted by NCIS to investigate and defeat the criminal threat posed to DON; responsible for NCIS efforts to reduce criminal activity and its impact on the U.S. Navy and U.S. Marine Corps.

(1) Exercises leadership of crime reduction efforts through NCIS Criminal Investigations Program Direction Document and exercises direction of it through the three field directorates; advises the Deputy Director on the three field directorate Executive Assistant Directors' performance in meeting criminal investigations program goals and objectives.

(2) Establishes criminal investigative and crime reduction priorities and performance requirements and directs the Criminal Investigative Directorate's strategic planning efforts. The program direction responds to the Director's Strategic Vision and the priorities and performance requirements established by the Deputy Director.

(3) Produces the Criminal Investigations Program Direction Document for the Deputy Director's review, concurrence, and presentation to the Director for ultimate approval.

c. Accountable to the Deputy Director for NCIS' success in achieving its criminal investigative and operational mission.

d. Accomplishes the criminal investigations mission by causing the three field directorates (Atlantic, Pacific and Global Operations) to initiate and aggressively conduct proactive operations; by requiring field components to recruit and employ high level sources to support those operations; by establishing quality standards and demanding quality in all criminal investigations, operations, and source handling; and by engaging in liaison activities with key and appropriate U.S. Government, foreign government, and private sector entities.

e. Provides the Executive Assistant Directors of the three field directorates with clear and consistent operational direction; an optimally resourced and geographically situated workforce

to execute that direction (in conjunction with the Principal Executive Assistant Director for Management & Administration); and regularly scheduled assessments and feedback on mission performance.

f. Roles and Responsibilities of the Executive Assistant Director for Criminal Investigations

(1) When directed, acts in the Deputy Director's absence.

(2) Executes Director- and Deputy Director-delegated authorities and powers.

(3) Provides leadership for the Criminal Investigations Program.

(a) Directs the crime reduction strategic planning process. Tasks the Assistant Director, Criminal Investigations Directorate with strategic planning activities and requirements.

(b) Informed by the Director's Strategic Vision and the priorities and performance requirements established by the Deputy Director, annually produces the NCIS Criminal Investigations Program Direction Document for the Deputy Director's review and the Director's ultimate approval. Establishes and communicates his/her strategic vision and priorities for the direction of NCIS crime reduction efforts to the Executive Assistant Directors of the three field directorates.

g. Oversees the activities of the Criminal Investigations Directorate Departments.

(1) Executes through direction to, and supervision of, the Assistant Director of the Criminal Investigations Directorate.

(2) Reviews and evaluates the Assistant Director and the Deputy Assistant Director's performance.

(3) Advises the Director, Deputy Director, and Principal Executive Assistant Director on key program and personnel decisions.

h. Directs Criminal Investigations Directorate Program Direction and Management Activities.

(1) Identifies the criminal threat posed to the DON by criminal activity and illicit criminal networks; addresses the threat by directing the three field directorates to take prioritized actions to defeat and mitigate the threat; identifies, acquires, and aligns program resources to achieve desired results; and leads program liaison engagement.

(2) Threat and Program Impact Activities

(a) Identifies and prioritizes criminal threats to be countered.

1. Identifies, defines, and understands the threat posed to or impacting the DON by criminal activities, criminal enterprises, and illicit networks.

2. Informs, and is informed by, the NCIS Annual Crime Report, the Director's Strategic Vision, and NCIS Strategic Guidance.

3. Informs the development of the Criminal Investigations Program Direction Document and, by consequence, the three field directorates' Field Office Tactical Plans.

(b) Evaluates whether program activity is having an impact in mitigating the threat; continually assesses, reviews, and evaluates program activity for adequacy and situational awareness of program health; and when warranted, makes changes to program activities to achieve desired impact.

1. Establishes program performance measures against desired effects (programmatic and individual).

2. Conducts formal program performance reviews and assessments.

3. Conducts DON and DoD stakeholder satisfaction surveys; monitors the three field directorates' customer satisfaction survey activities.

4. Issues program direction modifications to achieve desired impact and mitigation effects, as warranted by program reviews.

(3) Plans and Strategic Initiatives

(a) Establishes Criminal Investigations Program Direction and Program priorities; produces, in conjunction with the Management & Administration Directorate, strategic planning documents providing the three field directorates with direction and priorities.

(b) Identifies and constructs and monitors high-priority, effects-based strategic initiatives that drive the execution of the criminal investigations program priorities through tasking the three field directorates.

(4) Policy and Resources

(a) Establishes and produces, in conjunction with the Management & Administration Directorate, policy guidance and program standards to assist the three field directorates implementation of program direction and assigned activities.

(b) Identifies, validates, and justifies the resource (manpower, training, equipment) requirements needed to execute the Criminal Investigations Program direction and objectives; coordinates with the Management & Administration Directorate to acquire and align criminal investigations program resources.

(5) Liaison and Engagement. Establishes criminal investigations program outreach and engagement priorities to establish, enhance, and exert maximum influence; leads and oversees program liaison and engagements activities. Liaison focus areas include:

(a) Intra-agency - Within NCIS.

(b) Inter-agency - Within DoD, DON, Navy, and Marine Corps.

(c) Seat of Government.

(d) International Partners.

(e) Private Sector.

(6) Directs Criminal Investigations Directorate Investigations and Operations Oversight Activities

(a) Oversees Director's special interest investigations, high-level, strategic initiative operations, and high-level, sensitive sources against program-prescribed, agency-approved quality standards.

(b) Monitors NCIS headquarters and the three field directorates special interest investigations and operations for NCIS, DON, DoD and Seat of Government situational awareness and reporting; advises three field directorates (Atlantic, Pacific, and Global Operations) on course(s) of action, when appropriate or as directed by NCIS executive staff, to ensure consistency with program-prescribed, agency-approved quality standards.

(c) Initiates and directs criminal investigations program source validation activities.

(d) Participates under Criminal Investigations Program Direction/Management direction in program performance assessments of field investigative and operations activities.

(7) Engages executive-level communications, internally and externally, in order to advise and inform NCIS employees and stakeholders.

(a) Keeps the Director and Deputy Director informed on all major policy, and management and administrative matters.

(b) Articulates NCIS, Director's, and Deputy Director's policy positions and equities.

(c) Educates and influences stakeholders, resource sponsors, and liaison partners. Serve as the primary NCIS point of contact for matters under the Criminal Investigations Directorate purview.

(d) Shares information of value.

2-12. Executive Assistant Director for National Security

a. Serves as the Chief Executive Officer for the NCIS National Security Directorate.

b. Directs the activities conducted by NCIS to investigate and defeat the terrorism and foreign intelligence threats posed to DON; responsible for NCIS efforts to prevent terror activities targeting U.S. Navy and U.S. Marine Corps equities and protecting against the compromise of DON sensitive information and critical systems.

(1) Exercises leadership of NCIS combating terrorism and counterintelligence efforts through his/her NCIS National Security Program Direction Document and exercises his/her direction of it through the three field directorates. Advises the Deputy Director on the Executive Assistant Directors (Atlantic, Pacific, and Global Operations) performance in meeting national security program goals and objectives.

(2) Establishes NCIS national security priorities and performance requirements and directs NCIS National Security Directorate strategic planning efforts. The program direction responds to the Director's Strategic Vision and the priorities and performance requirements established by the Deputy Director.

(3) Produces the NCIS National Security Program Direction Document for the Deputy Director's review, concurrence, and presentation to the Director for ultimate approval.

c. Accountable to the Deputy Director for NCIS' success in achieving its combating terrorism and counterintelligence investigative and operational mission.

d. Accomplishes the NCIS national security mission by causing the three field directorates to initiate and aggressively conduct proactive operations and cyber activities; requiring field components to recruit and employ high level sources to support those operations and activities; by establishing quality standards and demanding quality in all NCIS national security investigations, operations, and source handling; and by engaging in liaison activities with key and appropriate U.S. Government, foreign government, and private sector entities.

e. Provides the Executive Assistant Directors of the three field directorates with clear and consistent operational direction; an optimally resourced and geographically-situated workforce to execute that direction (in conjunction with the Principal Executive Assistant Director for Management & Administration); and regularly scheduled assessments and feedback on mission performance.

f. Roles and Responsibilities of the Executive Assistant Director for NCIS National Security

(1) When directed, acts in the Deputy Director's absence.

(2) Executes Director- and Deputy Director-delegated authorities and powers.

(3) Provides leadership for the NCIS National Security Program.

(a) Directs the NCIS combating terrorism and counterintelligence strategic planning process. Tasks the Assistant Director, National Security Directorate with strategic planning activities and requirements.

(b) Informed by the Director's Strategic Vision and the priorities and performance requirements established by the Deputy Director, annually produces the NCIS National Security Program Direction Document for the Deputy Director's review and the Director's ultimate approval. Establishes and communicates his/her strategic vision and priorities for the direction of NCIS national security efforts to the three field directorates.

(4) Oversees the activities of the National Security Directorate Departments.

(a) Executes through direction to, and supervision of, the Assistant Director of the National Security Directorate.

(b) Reviews and evaluates Assistant Director and Deputy Assistant Directors' performance.

(c) Advises Director, Deputy Director, and Principal Executive Assistant Director on key program and personnel decisions.

(5) Directs National Security Directorate Program Direction and Management Activities

(a) Identifies the national security (terrorism, foreign intelligence, and cyber) threat posed to the DON by terrorist and espionage activities and international terror and intelligence networks; addresses the threat by directing the three field directorates to take prioritized actions to defeat and mitigate the threat; identifies, acquires, and aligns program resources to achieve desired results; and leads program liaison engagement.

(b) Threat and Program Impact Activities

1. Identifies and prioritizes national security threats to be countered.

2. Identify, define, and understand the threat posed to or impacting the DON by international terror and foreign intelligence activities and networks.

3. Informs, and is informed by, the NCIS Foreign Intelligence Threat to the DON, the Counterterrorism Report to the DON, the Director's Strategic Vision, and the NCIS Strategic Guidance.

(c) Informs the development of the National Security Program Direction Document and, by consequence, the three field Executive Assistant Directors' (Atlantic, Pacific, and Global Operations) Field Office Tactical Plans.

(d) Evaluates whether program activity is having an impact in mitigating the threat; continually assesses, reviews, and evaluates program activity for adequacy and situational awareness of program health; and when warranted, make changes to program activities to achieve desired impact.

1. Establishes program performance measures against desired effects; programmatic and individual.

2. Conducts formal program performance reviews and assessments.

3. Conducts DON and DoD stakeholder satisfaction surveys; monitors the three field directorates customer satisfaction survey activities.

4. Issues Program Direction modifications to achieve desired impact and mitigation effects, as warranted by program reviews.

(e) Plans and Strategic Initiatives

1. Establishes National Security Program Direction and Program priorities; produces, in conjunction with the Management & Administration Directorate, strategic planning documents providing the three field directorates with direction and priorities.

2. Identifies/constructs and monitors high-priority, effects-based strategic initiatives that drive the execution of National Security Program priorities through tasking of the three field directorates.

(f) Policy and Resources

1. Establishes and produces, in conjunction with the Management & Administration Directorate, policy guidance and program standards to assist the three field directorates implementation of program direction and assigned activities.

2. Identifies, validates, and justifies the resource (manpower, training, equipment) requirements needed to execute national security program direction and objectives; coordinates with the Management & Administration Directorate to acquire and align national security program resources.

(g) Liaison and Engagement. Establishes National Security Program outreach and engagement priorities to establish, enhance, and exert maximum influence; leads and oversees program liaison and engagements activities. Liaison focus areas include:

1. Intra-agency - Within NCIS.

2. Inter-agency - Within DoD, DON, Navy, and Marine Corps.

3. Seat of Government.

4. International Partners.

5. Private Sector.

(h) Directs National Security Directorate Investigations and Operations Oversight Activities.

1. Oversees Director's special interest investigations; high-level, strategic initiative operations; high-level, sensitive sources; and cyber/computer network activities against program-prescribed, agency-approved quality standards.

2. Monitors NCIS headquarters and the three field directorates special interest investigations and operations for NCIS, DON, DoD and/or seat of government situational awareness and reporting; advises the three field directorates on course(s) of action, when appropriate or as directed by NCIS executive staff, to ensure consistency with program-prescribed, agency-approved quality standards.

(i) Initiates and directs national security program source validation activities.

(j) Participates under National Security Program Direction/Management direction in program performance assessments of field investigative and operations activities.

(k) Engages executive-level communications, internally and externally, in order to advise and inform NCIS employees and stakeholders.

1. Keeps the Director and Deputy Director informed on all major policy and management and administrative matters.

2. Articulates NCIS, Director's, and Deputy Director's policy positions and equities.

3. Educates and influences stakeholders, resource sponsors, and liaison partners. Serve as the primary NCIS point of contact for matters under National Security Directorate purview.

4. Shares information of value.

2-13. Executive Assistant Directors for Atlantic and Pacific Operations

a. Serves as the NCIS executive for the execution of its mission execution responsibilities within a geographic area of responsibility or region.

b. Directs the activities conducted by subordinate NCIS field offices to investigate and defeat the terrorism, foreign intelligence, and criminal threats posed to the DON in the region; responsible for the day-to-day oversight and management of the NCIS and its activities, operational and administrative, within the sphere of his/her geographic area of responsibility.

(1) Exercises leadership of regional implementation of NCIS headquarters program goals and objectives through his/her Regional Performance Plan and exercises his direction of it through his/her supervision of the region's the appropriate field directorates (Atlantic or Pacific Operations) Special Agents in Charge.

(a) Advises program executives of regional equities to be considered during strategic planning and policy development.

(b) Advises the Deputy Director on NCIS headquarters Executive Assistant Director program management performance relative to his/her sphere of operations.

(2) Establishes regional NCIS operational priorities and performance requirements in collaboration with NCIS headquarters executives; directs the region's tactical response planning to program strategic planning documents. The Regional Performance Plan responds to the Director's Strategic Vision and the priorities and performance requirements of the Deputy Director and the NCIS headquarters program executives.

(3) Produces the region's performance plan in collaboration with the NCIS headquarters executives and through the Management & Administration Directorate, for the Deputy Director's review, concurrence, and presentation to the Director for ultimate approval.

c. Accountable to the Deputy Director for NCIS' success in achieving its investigative and operational missions in his/her geographic area of responsibility and the effective management of the region's administrative activities.

d. Responsible to the NCIS headquarters program executives for the region's success in achieving the NCIS programs' investigative and operational missions.

e. Accomplishes the NCIS investigative and operational missions by ensuring that regional field offices initiate and aggressively conduct proactive operations; recruit and employ high-level sources to support those operations; conduct investigations, operations, and source handling that meet or exceed agency quality standards; and engage in liaison activities with key and appropriate federal, state, local, and foreign government and private sector entities.

f. Roles and Responsibilities of the Executive Assistant Directors for Atlantic and Pacific Operations

(1) Represents the Director with senior DoD, DON, combatant command, U.S. law enforcement and intelligence community and foreign government officials in the region.

(2) Executes Director- and Deputy Director-delegated authorities and powers.

(3) Provides leadership for the region's field office and directorate personnel.

(a) Produces, in collaboration with the NCIS headquarters program executives through the Management & Administration Directorate, the Region's Performance Plan to

implement NCIS headquarters program direction, goals, and objectives as captured in the NCIS Program Direction Documents. The regional performance plan is informed by the Director's Strategic Vision, the priorities and performance requirements of the Deputy Director and the NCIS headquarters program executives, and the priority requirements of the region's U.S. Navy, U.S. Marine Corps, and Combatant Command, and Naval Component Commanders,

(b) Directs the region's tactical response planning process. Collaborates with the region's Special Agents in Charge and the NCIS headquarters Management & Administration Directorate during the life cycle of the planning process to produce the region's Field Office Tactical Plans and Plan modifications.

(c) Produces, as necessary, region-wide NCIS policy implementation guidance in consultation with the NCIS Chief of Staff and program executives.

(d) Supervises the Executive Assistant Director's staff.

(4) Oversees the activities of the region's field offices. Executes these activities through his/her direction to, and supervision of the field directorates (Atlantic, or Pacific Operations) Special Agents in Charge.

(a) Ensures that regional field office investigations, operations, and source handling are assessed against agency-approved standards for quality; are aligned against NCIS headquarters program and field directorate priorities; and that field activities meeting the criteria for Special Interest are identified and communicated to the NCIS headquarters for higher headquarters situational awareness and reporting.

1. Manages the formal, NCIS headquarters approved field directorate (Atlantic or Pacific Operations) performance assessment and quality assurance review program.

2. Manages the formal, NCIS headquarters-approved Field Directorate special interest investigation and operation program to identify, review, and report on Special Interest operational activities.

(b) Reviews and evaluates field directorate (Atlantic or Pacific Operations) Special Agents in Charge and Assistant Special Agents in Charge performance against NCIS headquarters and field directorate (Atlantic or Pacific Operations) priorities and objectives. Oversees the field directorate (Atlantic or Pacific Operations) field office management visit program.

(c) Monitors the utilization of resources allocated to the region to ensure maximum operational effectiveness against NCIS headquarters program and field directorate priorities.

(d) Produces, in coordination with the NCIS headquarters program executives, an annual report for the Director assessing the region's performance in meeting its mission responsibilities.

(5) Serves as the primary point of contact between the field offices and the NCIS headquarters executives; coordinates with NCIS headquarters programs the validation and prioritization of resource requests; facilitates NCIS headquarters program-level support for field activities; and ensures timely and accurate field office response to NCIS headquarters directives, instructions, and investigative and administrative data calls.

(6) Prepares the region's liaison and engagement plan; directs the region's Special Agents in Charge implementation of NCIS headquarters program and field directorate outreach and engagement priorities; and provides regional guidance to inform field office liaison and engagement planning. Liaison and engagement focus areas include:

(a) Intra-agency - Within NCIS.

(b) Inter-agency - Within DoD, DON, Navy, and Marine Corps.

(c) Federal, State, and Local Entities.

(d) International Partners.

(e) Private Sector.

(7) Engages executive-level communications, internally and externally, in order to advise and inform NCIS employees, customers, and stakeholders.

(a) Keeps the Director, Deputy Director, and NCIS program executives informed of all major regional issues, events, and potential impediments to the successful execution of the NCIS mission.

(b) Articulates NCIS, Director's, and Deputy Director's policy positions and equities.

(c) Educates and influences regional customers, stakeholders, resource sponsors, and liaison partners. Serve as the primary NCIS point of contact for operational and resource matters within the region.

(d) Identifies and shares information of value.

2-14. Executive Assistant Director for Global Operations

a. The NCIS executive responsible for accomplishing mission responsibilities within specified functional areas of responsibility.

b. Directs the specified activities conducted by subordinate NCIS field offices and activities to investigate and defeat the terrorism, foreign intelligence, and criminal threats posed to the DON; responsible for the day-to-day oversight and management of the NCIS activities, operational and administrative, within the sphere of his/her functional areas of responsibility.

(1) Exercises his direction through his/her supervision of the directorate's field office Special Agents in Charge.

(2) Advises program and field executives of directorate equities to be considered during strategic planning and policy development,

(3) Establishes performance requirements in collaboration with NCIS headquarters program and field executives; directs the field office Special Agents in Charge tactical response planning to program and field directorate strategic planning documents.

c. Accountable to the Deputy Director for NCIS' success in achieving its investigative and operational missions in his/her functional area of responsibility and the effective management of the directorate's administrative activities. Advises the Deputy Director, primarily through Management & Administration Directorate performance measures, on NCIS headquarters and field executive program management performance relative to his/her sphere of responsibility.

d. Responsible to the NCIS headquarters program executives for the directorate's success in achieving the NCIS programs' investigative and operational missions; responsible to field executives for the directorate's success in achieving its investigative and operational missions within field executives' geographic areas of responsibility.

e. Accomplishes the NCIS investigative and operational missions by ensuring that directorate field offices initiate and aggressively conduct proactive operations; recruit and employ high-level sources to support those operations; conduct investigations, operations, and source handling that meet or exceed agency quality standards; and engage in liaison activities with key and appropriate federal, state, local, and foreign government and private sector entities.

f. Accomplishes the NCIS investigative and operational mission by ensuring field operational support elements (Offices of Technical Support, Polygraph Services, Forensic Support, and TSCM) provide specialized, functional capabilities to facilitate the execution of the national security and criminal investigative missions.

g. Roles and Responsibilities of the Executive Assistant Director for Global Operations

(1) Represents the Director with senior DoD, DON, Combatant Command, U.S. law enforcement and intelligence community, and foreign government officials within the sphere of his functional areas of responsibility.

(2) Executes Director- and Deputy Director-delegated authorities and powers.

(3) Provides leadership for the directorate's personnel.

(a) Produces, with Management & Administration Directorate facilitation support, directorate performance priorities, goals, and objectives to guide subordinate Special Agents in Charge and the heads of support elements. The directorate plan is informed by the

Director's Strategic Vision, the priorities and performance requirements of the Deputy Director and the NCIS headquarters program executives, and the priority requirements of the region's U. S. Navy, U.S. Marine Corps, and Combatant Command, and Naval Component Commanders.

(b) Directs the field offices' tactical response planning process.

(c) Collaborates with the directorate's Special Agents in Charge and the NCIS headquarters Management & Administration Directorate during the life cycle of the planning process to produce the directorate's Field Office Tactical Plans and Plan modifications.

(d) Produces, as necessary, directorate-wide NCIS policy implementation guidance in consultation with the NCIS Chief of Staff and program executives.

(4) Oversees the activities of the directorate's field offices.

(a) Executes through direction to, and supervision of the field office Special Agents in Charge and heads of the field operational support elements.

1. Ensures that directorate field office investigations, operations, source handling, and operational support activities are assessed against agency-approved standards for quality; are aligned against NCIS headquarters program and field directorate priorities; and that field activities meeting the criteria for special interest are identified and communicated to the NCIS headquarters for higher headquarters situational awareness and reporting.

2. Manages the formal, NCIS headquarters approved directorate performance assessment and quality assurance review program.

3. Manages the formal, NCIS headquarters approved directorate special interest investigation and operation program to identify, review, and report on special interest operational activities.

(b) Reviews and evaluates field office Special Agent in Charge and Assistant Special Agent in Charge performance against NCIS headquarters and field directorate priorities and objectives.

1. Manages the directorate's field office management visit program.

2. Monitors the utilization of resources allocated to the directorate to ensure maximum operational effectiveness against NCIS headquarters program, field directorate, and global operations directorate priorities.

3. Produces, in coordination with the NCIS headquarters program executives, an annual report for the Director assessing the directorate's performance in meeting its mission responsibilities.

(5) Serves as the primary point of contact between the directorate field offices, support elements, and the NCIS headquarters and field executives; coordinates with NCIS headquarters programs the validation and prioritization of resource requests; facilitates NCIS headquarters program-level support for field activities; and ensures timely and accurate directorate field office response to NCIS headquarters directives, instructions, and investigative and/or administrative data calls.

(6) Prepares the directorate's liaison and engagement plan; directs the directorate Special Agents in Charge implementation of NCIS headquarters program and field directorate outreach and engagement priorities; and provides directorate guidance to inform field office liaison and engagement planning. Liaison and engagement focus areas include:

(a) Intra-agency - Within NCIS.

(b) Inter-agency - Within DoD, DON, Navy, and Marine Corps.

(c) Federal, State, and Local Entities.

(d) International Partners.

(e) Private Sector.

(7) Engages executive-level communications, internally and externally, in order to advise and inform NCIS employees, customers, and stakeholders.

(a) Keeps the Director, Deputy Director, NCIS program and field executives informed of all major issues, events, and potential impediments to the successful execution of the NCIS mission.

(b) Articulates NCIS, Director's, and Deputy Director's policy positions and equities.

(c) Educates and influences directorate customers, stakeholders, resource sponsors, and liaison partners. In collaboration with the field executives, serve as the primary NCIS point of contact for operational and resource matters within his/her functional areas of responsibility.

(d) Identifies and shares information of value.

2-15. Chief, Intelligence and Information Sharing Directorate

a. Serves as the Chief Executive Officer for the NCIS Intelligence and Information Sharing Directorate (DIIS).

b. Directs the activities conducted by NCIS to provide intelligence, analysis, and related products to better understand the terror, intelligence, cyber, and criminal threats posed to the

DON; responsible for the intelligence and related products used by NCIS to reduce terrorist, intelligence, cyber, and criminal activity and their impact on the U.S. Navy and U.S. Marine Corps.

(1) Exercises leadership of NCIS intelligence collection, analysis, and production efforts through his/her NCIS Intelligence Program Direction Document and exercises his direction of it through the headquarters programs and the three field directorates (Atlantic, Pacific and Global Operations). Advises the Deputy Director on the three field directorates Executive Assistant Director's (Atlantic, Pacific, and Global Operations) performance in meeting intelligence program goals and objectives.

(2) Establishes NCIS intelligence priorities and performance requirements and directs NCIS Intelligence Directorate strategic planning efforts. The program direction responds to the Director's Strategic Vision and the priorities and performance requirements established by the Deputy Director.

(3) Produces the NCIS Intelligence Program Direction Document for the Deputy Director's review, concurrence, and presentation to the Director for ultimate approval.

c. Accountable to the Deputy Director for NCIS' success in achieving its intelligence and intelligence support missions.

d. Accomplishes the NCIS intelligence mission by causing the NCIS program, and the three field directorates (Atlantic, Pacific and Global Operations) to initiate and aggressively conduct proactive operations; requiring field components to recruit and employ high level sources to support those operations; by establishing quality standards and demanding quality in all NCIS criminal investigations, operations, and source handling; and by engaging in liaison activities with key and appropriate U.S. Government, foreign government, and private sector entities.

e. Provides the Executive Assistant Directors of the program directorates and the three field directorates (Atlantic, Pacific and Global Operations) with clear and consistent operational direction; an optimally resourced and geographically-situated workforce to execute that direction (in conjunction with the Principal Executive Assistant Director for Management & Administration); and regularly scheduled assessments and feedback on mission performance.

f. Roles and Responsibilities of the Chief for Intelligence

(1) When directed, acts in the Deputy Director's absence.

(2) Executes Director- and Deputy Director-delegated authorities and powers.

(3) Provides leadership for NCIS Intelligence Collection, Analysis, and Support Programs.

(a) Directs the NCIS intelligence program strategic planning process. Tasks the Assistant Director, Intelligence Directorate with strategic planning activities and requirements.

(b) Informed by the Director's Strategic Vision and the priorities and performance requirements biennially produces the NCIS Intelligence Program Direction Document for the Deputy Director's review and the Director's ultimate approval. Establishes and communicates his/her strategic vision and priorities for the direction of NCIS intelligence collection, analysis, and intelligence support efforts to the headquarters programs and field executive assistant directors.

(4) Oversees the activities of the NCIS Intelligence Directorate.

(a) Executes DIIS mission objectives and responsibilities through direction to, and supervision of, assigned Deputy Assistant Directors .

(b) Reviews and evaluates Deputy Assistant Director performance.

(c) Advises the Director, Deputy Director, and Principal Executive Assistant Director on key program and personnel decisions.

(5) Directs Intelligence Directorate Program Direction and Management Activities

(a) Identifies the threats posed to the DON by international terrorist organizations, foreign intelligence services, and criminal activity and illicit criminal networks; addresses the threat by directing the program and field directorates to take prioritized actions to defeat/mitigate the threat; identifies, acquires, and aligns program resources to achieve desired results; and leads program liaison engagement.

(b) Threat and Program Impact Activities

1. Identifies and prioritizes international terrorist, foreign intelligence, and criminal threats to be countered.

a. Identify, define, and understand the threat posed to or impacting the DON by terrorist, intelligence, criminal activities, enterprises, and networks.

b. Informs the development of the Intelligence Program Direction Document and, by consequence, the Programs' Direction Documents, Field Executive Assistant Directors' Regional Priorities and Field Office Tactical Plans.

2. Evaluates whether program activity is having an impact in mitigating the threats; continually assesses, reviews, and evaluates program activity for adequacy and situational awareness of program health; and when warranted, make changes to program activities to achieve desired impact.

a. Establishes program performance measures against desired effects; programmatic and individual.

b. Conducts formal program performance reviews and assessments.

c. Conducts NCIS, DON, and DoD stakeholder satisfaction surveys; monitors program and the three field directors (Atlantic, Pacific and Global Operations) customer satisfaction survey activities.

d. Issues Program Direction modifications to achieve desired impact and mitigation effects, as warranted by program reviews.

(c) Plans and Strategic Initiatives

1. Establishes Intelligence Program Direction and Program priorities; produces, in conjunction with the Management & Administration Directorate, strategic planning documents providing the program and three field directorates (Atlantic, Pacific and Global Operations) with the direction and priorities.

2. Identifies and constructs and monitors high-priority, effects-based strategic initiatives that drive the execution of the Intelligence Program priorities through tasking of the program, field, and global operations directorates.

(d) Policy and Resources

1. Establishes and produces, in conjunction with the Management & Administration Directorate, policy guidance and program standards to assist program and the three field directorates (Atlantic, Pacific and Global Operations) implementation of program direction and assigned activities.

2. Identifies, validates, and justifies the resource (manpower, training, equipment) requirements needed to execute the Intelligence Program direction and objectives; coordinates with the Management & Administration Directorate to acquire and align intelligence program resources.

(6) Directs Global Engagement Activities

(a) Manages the overarching NCIS Global Engagement Program, including the production of the NCIS Global Engagement Strategy; establishes Intelligence Program outreach and engagement priorities to establish, enhance, and exert maximum influence; leads and oversees program liaison and engagements activities. Liaison focus areas include:

1. Intra-agency - Within NCIS (Internal to Directorate).

2. Inter-agency - Within DoD, DON, Navy, and Marine Corps.

3. Seat of Government.

4. International Partners.

5. Private Sector.

(b) Manages the NCIS Central Source Registry and oversees NCIS source deconfliction and coordination.

(7) Directs Intelligence Directorate Analysis Activities

(a) Strategic Analysis. Provides all-source analysis and situational awareness of potential terror, intelligence, or criminal threats and/or organizational vulnerabilities. Assesses the impact of emerging national security and criminal threats to the DON and NCIS' ability to respond.

(b) Operational Analysis. Provides all-source analytic support to program and three field directorates (Atlantic, Pacific and Global Operations) to identify program coverage gaps and opportunities; collaborates with the programs to identify specific gaps in their knowledge base of threats and adversaries.

(c) Tactical Analysis. Provides direct and time-sensitive analysis of tactical intelligence derived during ongoing NCIS investigations and operations. Leads NCIS source validation efforts.

(d) Operational Targeting. Collaborates with the operational programs to refine collection efforts to identify and target critical knowledge gaps; produces targeting packages that translates threat information into actionable intelligence.

(e) Collection Management. Oversees the prioritization of national, DoD, DON and NCIS information requirements; directs the headquarters program and the three field directorates (Atlantic, Pacific and Global Operations) to devise collection operations and recruit sources to fulfill these requirements.

(f) Production. Produces finished NCIS intelligence and analytical products including, but not limited to, threat assessments, maritime threat products, special analytic reports, and criminal intelligence briefs. Collaborates with the National Security and Criminal Directorates and produces the Foreign Intelligence Threat to the DON, the Terrorist Threat to the DON, and the Annual DON Crime Report.

(g) Indications and Warning. Manages the Multiple Threat Alert Center providing 24/7 dissemination of indications and warnings to the DON, NCIS, and the intelligence community. Provides tailored executive- and pre-deployment briefings, major event support, and forward deployed analytic support to DON and NCIS.

(8) Engages executive-level communications, internally and externally, in order to advise and inform NCIS employees and stakeholders.

(a) Keeps the Director and Deputy Director informed on all major policy and management and administrative matters.

(b) Articulates NCIS, Director's, and Deputy Director's policy positions and equities.

(c) Educates and influences stakeholders, resource sponsors, and liaison partners. Serve as the primary NCIS point of contact for matters under Intelligence Directorate purview.

(d) Shares information of value.

2-16. Chief, Financial Management and Planning

a. Serves as the Chief Executive Officer for the NCIS Financial Management and Planning Directorate.

b. Directs the activities conducted by NCIS to develop overarching agency strategies and to provide the program planning, evaluation, and performance assessment necessary to accomplish the strategic mission of NCIS in the near and long-term.

c. Responsible for ensuring that NCIS is adequately financed and that resources are spent lawfully and in accordance with NCIS executive policy decisions; for maintaining effective program planning and performance assessment processes which integrate operational planning and activities with budget, human resources, and facilities planning; and for providing timely and accurate security clearance adjudication and information security policy.

(1) Exercises leadership of NCIS fiscal and program planning and evaluation through his/her NCIS Financial Management & Planning Program Direction Document and exercises his/her direction of it through his/her day-to-day oversight and management of the Directorate's activities.

(2) Establishes NCIS fiscal and program planning priorities and performance requirements; directs NCIS Financial Management & Planning Directorate strategic planning and program planning support efforts.

(a) The Financial Management & Planning Program Direction responds to the Director's Strategic Vision, the priorities and performance requirements established by the Deputy Director, and the priorities and objectives of the Principal Executive Assistant Director for Management & Administration.

(b) Produces the NCIS Financial Management & Planning Program Direction Document for the Principal Executive Assistant Director's review, concurrence, and presentation to the Deputy Director.

d. Accountable to the Principal Executive Assistant Director for Management & Administration for the Directorate's success in meeting its fiscal and program planning and evaluation missions.

e. Responsible to the program executives to plan for and manage agency efforts to acquire fiscal resources necessary to meet validated mission requirements; to plan, implement, and maintain an effective strategic program planning process; and to facilitate the evaluation and monitoring of organization performance and impact.

f. Roles and Responsibilities of the Chief, Financial Management & Planning Directorate

(1) Acts in the Principal Executive Assistant Director's absence, when directed.

(2) Executes Principal Executive Assistant Director-delegated authorities and powers.

(3) Provides leadership for NCIS Financial Management & Planning activities.

(a) Directs the NCIS financial management and planning/evaluation strategic planning processes. Tasks the Deputy Assistant Directors and Department Heads with fiscal and strategic planning activities and requirements.

(b) Biennially produces the NCIS Financial Management & Planning Program Direction Document for the Principal Executive Assistant Director's review, concurrence, and presentation to the Deputy Director.

(4) Supervises, reviews, and evaluates Deputy Assistant Director, and Department Head performance.

(5) Advises Principal Executive Assistant Director on key program and personnel decisions.

(6) Oversees the activities of the Financial Management and Planning Directorate, specifically:

(a) Fiscal Planning and Management (Budget, Accounting, and Fiscal Analysis/Policy).

1. Produces the NCIS Strategic (Six Year) Budget.

2. Produces the NCIS Annual Budget.

a. Principally responsible for coordination with all NCIS resource sponsors.

b. Coordinates with NCIS Programs to identify and deconflict crosscutting issues.

c. Produces all financial documents required by resource sponsors.

(b) Prepares and produces the annual NCIS Financial Plan (Current Year Execution).

1. Ensures budgeted resources are allocated as directed by NCIS senior management.

2. Provides NCIS executives with periodic obligation and expenditure reporting.

3. Implements and maintains the NCIS accounting process; tracks and records all NCIS financial transactions; matches expenditures with appropriate obligations and accounts for exceptions; ensures compliance with all instructions and laws.

4. Prepares directorate-required financial analysis and supports NCIS programs with financial analysis when requested.

(c) Planning and Evaluation

1. Coordinates the development and production of NCIS strategic and program planning documents and performance assessments.

2. Directs the NCIS Strategic Management/Mission Performance Analysis Process.

a. Collaborates with the programs to develop performance targets, measures, and metrics that will facilitate performance assessment.

b. Facilitates periodic program performance reviews.

c. Prepare, coordinate, or lead program evaluations, impact studies, and research, as requested; provide program executives with recommendations resulting from evaluative effort.

(d) Engages executive-level communications, internally and externally, in order to advise, inform, and influence NCIS employees, customers, stakeholders, and partners.

1. Keeps the Director, Deputy Director, the Principal Executive Assistant Director, and NCIS Executives informed on all matters pertaining to financial management, program planning and evaluation, DON clearance adjudication, and DON information security.

2. Articulates NCIS, Director, Deputy Director, and Principal Executive Assistant Director policy positions and equities.

3. Educates and influences stakeholders, resource sponsors, and liaison partners.

4. Shares information of value.

2-17. Assistant Director, Human Resources

a. Serves as the Chief Executive Officer for the NCIS Human Resources Directorate.

b. Directs the activities conducted by NCIS to recruit, develop, and retain a workforce capable of accomplishing the strategic mission of NCIS in the near- and long-term; responsible for NCIS business operations that produce a knowledgeable, well-trained, motivated, and optimally-located workforce, from entry- through executive- levels.

(1) Exercises leadership of NCIS human capital development and workforce planning efforts through his/her NCIS Human Resources Program Direction Document and exercises his/her direction of it through his/her day-to-day oversight and management of the Directorate's activities.

(2) Establishes NCIS human capital development and workforce planning priorities and performance requirements; directs NCIS Human Resources Directorate strategic planning efforts.

(a) Human Resources Program Direction responds to the Director's Strategic Vision, the priorities and performance requirements established by the Deputy Director, and the priorities and objectives of the Principal Executive Assistant Director for Management & Administration.

(b) Produces the NCIS Human Resources Program Direction Document for the Principal Executive Assistant Director's review, concurrence, and presentation to the Deputy Director.

c. Accountable to the Principal Executive Assistant Director for Management & Administration for the directorate's success in meeting its human capital development and workforce planning mission.

d. Responsible to the program and field executives to acquire and align workforce resources to meet validated mission requirements.

e. Roles and Responsibilities of the Assistant Director, Human Resources

(1) When directed, acts in the Principal Executive Assistant Director's absence.

(2) Executes Principal Executive Assistant Director-delegated authorities and powers.

(3) Provides leadership for NCIS Human Capital Development and Workforce Planning Activities.

(a) Directs the NCIS human resources strategic planning process. Tasks the Deputy Assistant Directors and Department Heads with strategic planning activities and requirements.

(b) Biennially produces the NCIS Human Resources Program Direction Document for the Principal Executive Assistant Director's review, concurrence, and presentation to the Deputy Director.

(4) Supervises, reviews, and evaluates Deputy Assistant Director and Department Head performance.

(5) Advises Principal Executive Assistant Director on key program and personnel decisions.

(6) Oversees the activities of the Human Resources Directorate, specifically:

(a) Human Resources Operations & Services (Personnel Services, Benefits, and Employee Relations.)

1. Position Management and Classification. Collaborates with NCIS programs to identify job series, and positions needed to meet mission-related functions; prepares position descriptions which detail the required knowledge, skills, and abilities; develops career paths and succession planning guidance to assist employee career advancement efforts.

2. Personnel Benefits and Processing and Employee Relations. Facilitates and administers established federal and military program benefits and services to NCIS employees, including pay and benefits, retirement counseling and processing, worker's compensation program, and the grievance and disciplinary program.

3. Performance Management. Administers and provides direction for the NCIS performance appraisal and awards process; collaborates with NCIS supervisors to develop competency-based performance plans that link performance expectations with agency goals; and advises supervisors addressing performance deficiencies.

(b) Training

1. Strategic and Operational Planning. Collaborates with the programs and three field directorates (Atlantic, Pacific and Global Operations) and produces agency-wide training needs assessments, training plans, and training strategies.

2. New Agents' Training Program. Oversees the development and delivery of a training program that provides new special agents with the requisite knowledge, skills, and abilities. Ensures that training is delivered by qualified instructors and meet training certification standards.

3. Specialized Investigative/Operational Training. Responsible, with collaboration from the program, field, and global directorates, for identifying, developing, acquiring, and delivering advanced investigative and operational courses of instruction that meet the prioritized needs of the NCIS.

4. Professional Staff and Support Staff Training. Ensures the job-related training needs, specialized training, and career development needs of the NCIS professional and support staff personnel are addressed.

5. Provide required support to the Federal Law Enforcement Training Center.

(c) Human Capital Development

1. Workforce Planning. With collaboration from the NCIS program and the three field directorates (Atlantic, Pacific and Global Operations) produces and directs the execution of the NCIS Workforce Development Strategy.

2. Assesses and addresses NCIS special agent, professional staff, and support staff development, recruitment, retention, and development requirements, based on near term staffing needs and projected future skill needs.

(d) Leadership Development and Executive Succession Planning

1. Manages the NCIS Leadership Development Program (Levels I & II).

2. Coordinates NCIS Senior Leader Training.

3. Provides Executive Succession Planning support.

(e) Engages executive-level communications, internally and externally, in order to advise, inform, and influence NCIS employees, customers, stakeholders, and partners.

1. Keeps the Director, Deputy Director, the Principal Executive Assistant Director, and NCIS executives informed on all matters pertaining to workforce development and planning, human resources actions, policies, and workforce training.

2. Articulates NCIS, Director, Deputy Director, and Principal Executive Assistant Director policy positions and equities.

3. Educates and influences stakeholders, resource sponsors, and liaison partners.

4. Shares information of value.

2-18. Assistant Director, Administration & Logistics

a. Serves as the Chief Executive Officer for the NCIS Administration & Logistics Directorate.

b. Directs the activities conducted by NCIS to enable the execution of its strategic mission, both in the near- and long-term, with facilities management, procurement management, logistics and supply management, security management, records management, and administrative services support; responsible for NCIS business operations that ensure a highly efficient administrative and logistics support program.

(1) Exercises leadership of NCIS administrative and logistics efforts through his/her NCIS Administration and Logistics Program Direction Document and exercises his/her direction of it through his/her day-to-day oversight and management of the Directorate's activities.

(2) Establishes NCIS facilities, logistics, security, procurement, and administrative support management planning priorities and performance requirements; directs NCIS Administration and Logistics Directorate strategic planning efforts.

(a) The Administration and Logistics Program Direction responds to the Director's Strategic Vision, the priorities and performance requirements established by the Deputy Director, and the priorities and objectives of the Principal Executive Assistant Director for Management & Administration.

(b) Produces the NCIS Administration and Logistics Program Direction Document for the Principal Executive Assistant Director's review, concurrence, and presentation to the Deputy Director.

c. Accountable to the Principal Executive Assistant Director for Management & Administration for the Directorate's success in meeting its facilities, procurement, security, logistics, and administrative management mission.

d. Responsible to the program and field executives for suitable and properly maintained facilities; for clear and consistent security programs, policy, and training; for agile and responsive logistics and procurement business operations that ensure the timely acquisition and delivery of equipment and services; and for an agile administrative support program that enables timely NCIS-wide staff action resolution, timely NCIS policy guidance, and effective records management.

e. Roles and Responsibilities of the Assistant Director, Administration & Logistics

(1) When directed, acts in the Principal Executive Assistant Director's absence.

(2) Executes Principal Executive Assistant Director-delegated authorities and powers.

(3) Provides leadership for NCIS facilities management, logistics and supply, security management, contracting & procurement, and administrative support service activities.

(a) Directs the NCIS Administration and Logistics strategic planning process; tasks the Deputy Assistant Directors and Department Heads with strategic planning activities and requirements.

(b) Biennially produces the NCIS Administration and Logistics Program Direction Document for the Principal Executive Assistant Director's review, concurrence, and presentation to the Deputy Director.

(4) Supervises, reviews, and evaluates Deputy Assistant Director and Department Head performance.

(5) Advises the Principal Executive Assistant Director on key program and personnel decisions.

(6) Oversees the activities of the Administration and Logistic Directorate, specifically:

(a) Security and Facilities. Physical, Personnel, Information, and Special Security Management. Manages the full-scope security program for NCIS, covering physical, personnel, information, and special security issues; produces security policy for NCIS processing and adjudication of personnel security clearances, maintaining control of special security sources and documents, and maintaining the physical security of NCIS facilities and spaces.

(b) Manages the NCIS Credential and Badge Program.

(c) Security Management Training Program. Provides/provides for security training for all agency personnel; uses the full spectrum of communications/media methods to instruct NCIS employees on proper handling of protected materials, classified information, and equipment.

(d) Facilities Engineering and Planning Management.

1. Manages NCIS facility and real property maintenance; participates in the planning, programming, and budgeting process to ensure adequate funding for facility acquisition, replacement, improvement, repair, or alteration; coordinates the resolution of technical facilities engineering issues with local commands and/or real property managers; and prepares engineering plans for facility improvement or repair and oversees contracted architectural and/or engineering support.

2. Produces and publishes an annual facilities plan detailing NCIS facility requirements for the year of execution, and projecting major facilities requirements for the following year; conducts surveys to determine mid- and long-term facility requirements; coordinates with DON property management entities to ensure NCIS facility requirements receive priority consideration for unimpeded law enforcement at naval installations.

(e) Acquisition and Logistics.

1. Manages all NCIS contracting and procurement activities; facilitates program source selection and other contracting decision-making; produces NCIS procurement documentation; coordinates agency purchase actions with the end-user to ensure propriety and timeliness; maintains the agency's acquisition record management system; and develops and publishes policy and procedure governing the NCIS acquisition including the issuance and use of agency purchase cards.

2. Manages NCIS logistics programs for vehicles, fuel, weapons, ammunition, accountable property, and criminal investigative supplies; maintains the agency's vehicle, arms, and ammunition record management and reporting programs; and develops and publishes policy and procedures governing NCIS logistics.

(f) Administrative Services.

1. Staff Action Management. Responsible for the Executive Decision Making Process (EDMP); collaborates with the headquarters program directorates and the three field directorates to produce actionable EDMP packages; and administers the NCIS application of the SECNAV Tasker System.

2. Policy Maintenance. Maintains official records of all current policy documents, manuals; manages the agency's periodic policy review and update process.

3. Correspondence Control. Responsible for tracking and fulfilling incoming and outgoing correspondence action, policy, directives review, action taskers, and other requests for information.

4. Records Management and Disposal. Manages the DON central repository for closed law enforcement, counterterrorism, and counterintelligence investigative and operational records; responds to requests for investigative records by federal, state, and local government agencies; ensures compliance with departmental record management directives and requirements; and prepares agency policy for records creation and management.

5. Community Management. Administers community management responsibilities for NCIS administrative support personnel.

(7) Engages executive-level communications, internally and externally, in order to advise, inform, and influence NCIS employees, customers, stakeholders, and partners.

(a) Keeps the Director, Deputy Director, the Principal Executive Assistant Director, and NCIS executives informed on all matters pertaining to facilities, logistics, and administrative support.

(b) Articulates NCIS, Director, Deputy Director, and Principal Executive Assistant Director policy positions and equities.

(c) Educates and influences stakeholders, resource sponsors, and liaison partners.

(d) Serves as the primary NCIS liaison within NCIS and with the DON, DoD, and other agencies regarding facilities, procurement, security, and records management and administrative services.

(e) Shares information of value.

2-19. Assistant Directors (Criminal & National Security Directorates)

a. Serves as the Chief Operating Officer for the Directorate.

b. Responsible for the day-to-day oversight and management of the Directorate's activities; supervises directorate activities to prevent or reduce threats targeting DON equities.

(1) Manages the execution of NCIS mission responsibilities through the Directorate's Program Direction Document and facilitates it through the three field directorates.

(2) Manages the Directorate's strategic planning efforts.

(3) Oversees the development and production of the Directorate's Program Direction Document for the Executive Assistant Director's review and approval for presentation to the Deputy Director.

c. Accountable to the Executive Assistant Director for the Directorate's success in meeting its investigative and operational mission and the effective management of its administrative activities, including the production of clear and consistent operational direction; an optimally resourced and geographically-situated workforce to execute that direction (in conjunction with the NCIS Financial Management & Planning Directorate); and regularly scheduled assessments and feedback on mission performance.

d. Roles and Responsibilities of the Assistant Director (Criminal & National Security Directorates.)

(1) Acts in the Executive Assistant Director's absence.

(2) Executes Executive Assistant Director-delegated authorities and powers.

(3) Supervises, reviews, and evaluates Deputy Assistant Director performance.

(4) Advises Executive Assistant Director on key program and personnel decisions.

(5) Manages the day-to-day activities of the Directorate, specifically:

(a) Directorate's Program Direction and Management Activities

1. Threat and Program Impact.

a. Identifies and prioritizes the threats to be countered/mitigated.

b. Evaluates whether program activity is impacting threat mitigation; continually assesses, reviews, and evaluates program activity for adequacy and situational awareness of program health; and when warranted, makes changes to program activities to achieve desired impact.

2. Plans and Strategic Initiatives.

a. Establishes Program Direction and Program priorities; produces, in conjunction with the Planning and Evaluation Department, strategic planning documents to guide field and global operations directorate efforts.

b. Identifies/constructs and monitors high-priority, effects-based strategic initiatives that drive the field and global operations directorates' execution of Program priorities.

3. Policy and Resources.

a. Establishes and produces, in conjunction with the Management & Administration Directorate, policy guidance and program standards to guide field implementation of program direction and assigned activities.

b. Identifies, validates, and justifies the resource (manpower, training, equipment) requirements needed to execute Program direction and objectives

c. Coordinates with the Management & Administration Directorate to acquire and align program resources.

(b) Liaison and Engagement. Establishes program outreach and engagement priorities to establish, enhance, and exert maximum influence. Liaison focus areas include:

1. Intra-agency - Within NCIS

2. Inter-agency - Within DoD, DON, United States Navy, and Marine Corps

3. Seat of Government

4. International Partners

5. Private Sector

(c) Directorate's Investigations and Operations Oversight Activities

1. Oversees Director's Special Interest investigations; high-level, strategic initiative operations and activities; and high-level, sensitive sources against Program-prescribed, agency-approved quality standards.

2. Monitors NCIS headquarters and field, and global operations directorate special interest investigations, operations, and activities for NCIS, DON, DoD, and Seat of Government situational awareness and reporting; advises the three field directorates elements on course(s) of action, when appropriate or when directed by higher authority, to ensure consistency with program-prescribed, agency-approved quality standards.

3. Initiates program source validation activities.

4. Ensures Investigation and Operation Department participation in the Directorate's performance assessment of field investigative and operations activities.

2-20. Assistant Director, Information Technology

a. Serves as the NCIS Command Information Officer; principal advisor to the Director for issues regarding information management and alignment of information technology (IT) investments to business priorities and assigned missions.

b. Serves as the Chief Executive Officer for the NCIS Information Technology Directorate.

c. Directs the activities conducted by NCIS to plan, implement, and maintain the NCIS IT infrastructure necessary to accomplish the strategic mission of NCIS in the near- and long-term; responsible for the effective use of NCIS information resources across the organization to successfully meet its goals and objectives and for NCIS business operations that enable the design, development, procurement, operation, and maintenance of NCIS information systems.

(1) Exercises leadership of NCIS information resources management through his/her NCIS Information Technology Program Direction Document and exercises his/her direction of it through his/her day-to-day oversight and management of the Directorate's activities.

(2) Establishes NCIS information resources management priorities and performance requirements; directs NCIS Information Technology Directorate strategic planning efforts.

(a) Information Technology Program Direction responds to the Director's Strategic Vision, the priorities and performance requirements established by the Deputy Director, and the priorities and objectives of the Principal Executive Assistant Director for Management & Administration.

(b) As directed and aligned with the NCIS Strategic Plan, produces for the Principal Executive Assistant Director's review, concurrence, and presentation to the Deputy Director, a multiyear NCIS Information Technology Strategic Plan that guides NCIS information resources management direction. Updates the IT Strategic Plan biennially.

(3) Produces the NCIS Information Technology Program Direction Document for the Principal Executive Assistant Director's review, concurrence, and presentation to the Deputy Director.

d. Accountable to the Principal Executive Assistant Director for Management & Administration for the Directorate's success in meeting its information management mission.

e. Responsible to the program and the three field directorates executives to develop, acquires, align, and maintain information systems and technologies to meet validated mission requirements.

f. Roles and Responsibilities of the Command Information Officer and Chief, Information Technology Directorate

(1) As Command Information Officer, serves as the Director's principal advisor regarding information resources management and IT investment.

(2) As the Directorate Chief, acts in the Principal Executive Assistant Director's absence, when directed.

(3) Executes Principal Executive Assistant Director-delegated authorities and powers.

(4) Provides Leadership for NCIS Information Management Activities

(a) Directs the NCIS information management and technology strategic planning process. Tasks the Deputy Assistant Directors/Department Heads with strategic planning activities and requirements,

(b) At higher direction, produces a multiyear NCIS Information Technology Strategic Plan, updated on a biennial basis that guides the design, development, procurement, and operation of NCIS information management systems and technologies.

(c) Biennially produces the NCIS Information Technology Program Direction Document for the Principal Executive Assistant Director's review, concurrence, and presentation to the Deputy Director.

(5) Supervises, reviews, and evaluates Deputy Assistant Director, and Department Head performance.

(6) Advises Principal Executive Assistant Director on key program and personnel decisions.

(7) Oversees the activities of the Information Technology Directorate, specifically:

(a) Information Technology Planning

1. In alignment with the NCIS Strategic Plan, produces a NCIS IT Strategic Plan, providing NCIS information resources management direction; updates the plan on a biennial basis.

2. Establishes Information Technology Program Direction and Program priorities; produces, in conjunction with the Planning and Evaluation Department, strategic planning documents providing support to the program and field directorates.

3. Develop an annual IT resource plan for inclusion into NCIS budget submissions to external stakeholders and resource sponsors.

(b) Performance Measures and Management. In collaboration with the Planning and Evaluation Department, establish and implement metrics to assess and report the value of IT investments.

(c) Enterprise Architecture Development and Implementation

1. Develop, implement, and maintain the technical and system views of the NCIS enterprise architecture; collaborate with the program executives to develop the operational view of the enterprise architecture.

2. Identify authoritative sources of NCIS enterprise data; formalize authoritative data sources through the architecture process.

3. Participate in DON Functional Area Manager activities and related DON application rationalization efforts; represent NCIS equities within these processes.

4. Chair the NCIS Architecture Review Board to ensure projects and investments are consistent with NCIS enterprise architecture; review and approve changes and updates to enterprise architecture.

5. Manage the NCIS IT Capital Planning and Investment Control process; chair the NCIS IT Investment Review Board.

(d) Technology Strategy Development.

(e) Information Resources Management Policy and Guidance.

(f) Central Design Activity. Manage requirements definition, systems design, modeling, development testing, integration, and implementation support.

(g) Enterprise Management

1. Acquire, manage, and support NCIS network and communications systems.

2. Operate and maintain the NCIS Data Center; provide data management services to NCIS applications, systems, and operations.

3. Manage application and system development, systems engineering, and system integration activities related to NCIS-owned and NCIS-administered applications.

4. Develop and execute risk-based continuity of operations planning for all NCIS-owned systems, applications, data, and infrastructure.

(h) Information Assurance and Security. Develop and implement NCIS information assurance strategies, plans, policies, and best practices.

(i) Engages executive-level communications, internally and externally, in order to advise, inform, and influence NCIS employees, customers, stakeholders, and partners.

1. Keeps the Director, Deputy Director, the Principal Executive Assistant Director, and NCIS executives informed on all matters pertaining to information management, information systems, and technology.

2. Articulates NCIS, Director, Deputy Director, and Principal Executive Assistant Director policy positions and equities. As the Command Information Officer, serves as the primary NCIS liaison with the DON Chief Information Officer, DON, DoD, and other agencies on matters pertaining to information management.

3. Educates and influences stakeholders, resource sponsors, and liaison partners.

4. Shares information of value.

(8) Supervises, reviews, and evaluates Deputy Assistant Director (DAD) performance.

2-21. Deputy Assistant Directors

a. Serves as the head of a programmatic department within a particular directorate.

b. Responsible for supervising, managing, and executing the department's activities. Dependent on the department's specific focus, these responsibilities include:

(1) Directs and executes oversight to ensure consistent quality and operational excellence of SI/DSI investigations and, in collaboration with the Field-EAD staffs and SACs, enterprise investigations and operations.

(2) Informs and advises through subject matter expertise relative to the organization, allocation, and alignment of resources to mitigate threat and address operational and organizational priorities.

(a) Provides information and advise relative to the directorate's Program Direction Document, re-evaluating as necessary in response to emerging requirements.

(b) Develops metric standards and monitor performance to assess and evaluate program and operational effectiveness; make adjustments as necessary to improve overall effectiveness.

(c) Makes recommendations pertaining to resource allocation and placement based on metrics-driven assessments, ensuring senior NCIS leadership remains aware of assumed risks associated with resource constraints or misalignment.

(3) Executes the department's strategic planning, management, and administrative efforts by implementing the Program's "Man, Train, and Equip" mission and providing support services.

(4) Exchanges information and collaborates with internal and external entities in furtherance of mission objectives. Liaison and engagement focus areas include:

(a) Intra-agency - Within NCIS.

(b) Inter-agency - Within DoD, DON, U.S. Navy, and U.S. Marine Corps.

(c) Federal, State, and Local Entities.

(d) International Partners, as appropriate.

(e) Private Sector.

(5) Accountable to the department's senior managing official for successfully meeting mission requirements and managing administrative activities.

c. Roles and Responsibilities of the Deputy Assistant Director

1. Acts in the absence of the department's senior managing official.

2. Executes delineated department functions and activities.

3. Supervises, reviews, and evaluates department staff performance.

4. Advises the department's senior managing official on key program and personnel decisions.

5. Continually assesses, reviews, and evaluates activities; takes appropriate actions to achieve the desired outcomes.

6. Evaluates activities for impact on threat mitigation, operational efficiency, and overall effectiveness.

7. Manages the day-to-day responsibilities of the department by identifying threats, prioritizing activities, and adjusting resources as necessary.

8. Executes EAD/AD-delegated authorities and powers.

9. Provides leadership for department personnel.

2-22. Special Agents in Charge

a. Serves as the senior NCIS manager responsible for the execution of agency mission responsibilities within a geographic or functional area of responsibility.

b. Directs the activities conducted by subordinate Field Office squads, NCIS resident agencies, and units to investigate and defeat the terrorism, foreign intelligence, and criminal threats posed to the DON within its area of responsibility; responsible for the day-to-day oversight and management of the NCIS and its activities, operational and administrative, within the sphere of his/her geographic or functional area of responsibility.

(1) Directs activity and executes oversight to ensure consistent quality and effectiveness of all assigned investigations and operations in collaboration with the Field-EAD staffs and program DADs.

(2) Exercises leadership of geographic and functional implementation of NCIS headquarters and field operations executive goals and objectives through his/her direction to and his/her supervision of the offices Assistant Special Agents in Charge and supervisory personnel. Advises program and field executive of local/regional equities to be considered during strategic planning and policy development.

(3) Produces NCIS field office operational priorities and performance requirements in collaboration with NCIS headquarters, and field and global operations; directs the office's tactical response planning to Program strategic planning documents. Field Office Tactical Plan responds to the Director's Strategic Vision and the priorities and performance requirements of the Deputy Director, the NCIS headquarters program, and field and global operations executive.

(4) Produces the Field Office Tactical Plan in collaboration with the NCIS headquarters, and field and global operations executive, through the Management & Administration Directorate, for the Deputy Director's review, concurrence, and presentation to the Director for ultimate approval.

c. Accountable to the field Executive Assistant Director for NCIS' success in achieving its investigative and operational mission in his/her geographic or functional area of responsibility and for the effective management of the field office's administrative activities.

d. Responsible to the field Executive Assistant Director for the field office's success in achieving the NCIS programs' investigative and operational missions.

e. Accomplishes the NCIS investigative and operational missions by ensuring that field office subordinate offices initiate and aggressively conduct proactive operations; recruit and employ high-level sources to support those operations; conduct investigations, operations, and source handling that meet or exceed agency quality standards; and engage in liaison activities with key and appropriate federal, state, local, and foreign government and private sector entities.

f. Roles and Responsibilities of the NCIS Field Office Special Agents in Charge

(1) Oversees the day-to-day activities of the field office, its squads, resident agencies, and units. Executes through direction to, and supervision of his/her Assistant Special Agents in Charge and supervisory personnel.

(2) Ensures that field office investigations, operations, and source handling are assessed against agency-approved standards for quality; are aligned against NCIS headquarters program, and field directorate priorities; and that field office activities meeting the criteria for special interest are identified and communicated to the field and global operations directorate executive and/or NCIS headquarters for higher headquarters situational awareness and reporting.

(3) Manages the formal, NCIS headquarter approved case review program throughout the field office.

(4) Reviews and evaluates field office supervisory personnel performance against NCIS headquarters, field and global directorate, and field office priorities and objectives.

(5) Executes the field operations directorates' Field Office Management Visit Program.

(6) Monitors the utilization of resources allocated to the field office to ensure maximum operational effectiveness against NCIS headquarters program, and the field operations directorate and field office priorities.

(7) Provides input as required to the appropriate field operations directorate executive to support an annual report for the Director assessing the region's performance in meeting its mission responsibilities.

(8) Represents the Director, and the field and global operations executive with senior DoD, DON, combatant command, U.S. law enforcement and intelligence community, and foreign government officials in geographic area of responsibility or the sphere of functional responsibility.

(9) Executes the field and global executive-delegated authorities and powers.

(10) Provides leadership for field office personnel.

(a) Produces, in collaboration with the NCIS headquarters and the appropriate field or global operations executives through the Management & Administration Directorate, the Field Office Tactical Plan to implement NCIS headquarters programs, and the field and global operations executive direction, goals, and objectives as captured in the NCIS Program Direction Documents and Regional Performance Plans. Informed by the Director's Strategic Vision, the priorities and performance requirements of the Deputy Director and the NCIS headquarters program executives, and the priority requirements of the region's U.S. Navy, U.S. Marine Corps, and Combatant Command and Naval Component Commanders.

(b) Directs the field office's tactical response planning process. Collaborates with the NCIS headquarters programs, the field directorate executives, and the NCIS headquarters Management & Administration Directorate during the life cycle of the planning process to produce the Field Office's Tactical Plan and Plan modifications.

(c) Produces, as necessary, field office-wide NCIS policy implementation guidance in consultation with the NCIS Chief of Staff and program executives.

(5) Serves as the primary point of contact between the field office subordinate offices and the field operations directorate Executive Assistant Director; provides input as required to support executive coordination for validation and prioritization of resource requests with NCIS headquarters programs executives; supports the field operations directorate executive facilitation of the NCIS headquarters program-level support for field office activities; and ensures timely and accurate field office response to NCIS headquarters directives, instructions, and investigative and administrative data calls via the field operations executive.

(6) Provides input as required to the field directorate executive to support his/her preparation of the region's liaison and engagement plan; directs the field office Assistant Special Agents in Charge and Supervisory Special Agents' implementation of NCIS headquarters program, and field directorate, and field office outreach and engagement priorities; and provides field office guidance to inform subordinate office liaison and engagement planning. Liaison and engagement focus areas include:

(a) Intra-agency - Within NCIS.

(b) Inter-agency - Within DoD, DON, U.S. Navy, and U.S. Marine Corps.

(c) Federal, State, and Local Entities.

(d) International Partners, as appropriate.

(e) Private Sector.

(7) Engages executive-level communications, internally and externally, in order to advise and inform NCIS employees, customers, and stakeholders.

(a) Keeps the Director, Deputy Director, and NCIS program executives informed via the field operations executive of all major regional issues, events, and potential impediments to the successful execution of the NCIS mission.

(b) Articulates NCIS, Director's, Deputy Director's, and the field operations executive policy positions and equities.

(c) Educates and influences regional customers, stakeholders, resource sponsors, and liaison partners. Serve as the primary NCIS point of contact for operational and resource matters within the field office geographic and functional area of responsibility.

(d) Identifies and shares information of value.

2-23. Chief of Staff

a. Serves as the Chief Administrative Officer for the Office of the Director (encompassing the Director, Deputy Director, Executive Assistant Directors, and the Director's Staff.)

b. Directs the day-to-day business operations of the Office of the Director; responsible for NCIS efforts to effectively administrate the actions requiring Director, NCIS decision or release authority; ensures that staff actions requiring executive decision are relevant, germane, timely, responsive, complete, and fully and appropriately vetted; and coordinates the flow of staff actions within the Office of the Director.

c. Accountable to the Director via the daily supervision of the Deputy Director for the effective operation and administration of the Office of the Director.

d. Accomplishes the effective operation and administration of the Office of the Director by causing the program directorates and each of the three field directorates executives and their staffs/elements to initiate and produce timely, fully-researched, and professionally-crafted staff action packages for executive staff consideration; causing the Director's staff and program directorates, and each of the three field directorates executives to review, vet, and provide relevant program-related commentary on pending staff actions for Director and/or Deputy Director consideration; and by recommending resolutions or courses of action for the Director and/or Deputy Director.

e. Roles and Responsibilities of the Chief of Staff

(1) Executes specified Director and Deputy Director-delegated authorities and powers.

(2) Supervises, reviews, and evaluates selected Office of the Director staff performance.

(3) Advises the Director and Deputy Director on key staff and executive decision-required actions.

(4) Directs the business operations of the Office of the Director. The Office of the Director requirements are executed through his/her collaboration with the Director's Staff and the program, and the field directorates (Atlantic, Pacific, and Global Operations) executives responsible for the development and production of staff actions and staff action-related activities.

(5) Coordinates the submission of policy-related (development, coordination, review, and/or de-confliction) action packages for Director and/or Deputy Director considerations; reviews submissions and makes recommendations to the Deputy Director.

(6) Oversees the execution of Director and Deputy Director-tasked special projects.

(7) Engages executive-level communications, internally and externally, in order to advise and inform NCIS employees and stakeholders.

(a) Articulates NCIS, Director's, and Deputy Director's policy positions and equities.

(b) Educates and influences stakeholders, resource sponsors, and liaison partners.

(c) Shares information of value.

2-24. Communications Director

a. Serves as the principal advisor to the Director for issues regarding NCIS interaction with the NCIS workforce, the Congress, the media, and the public.

b. Supervises the NCIS Office of Communications.

c. Directs the activities conducted by NCIS to plan, implement, and maintain the liaison outreach necessary to communicate the strategic mission and activities of NCIS; responsible for the effective use of NCIS communications and liaison resources across the organization to successfully meet its goals and objectives.

(1) Exercises leadership of NCIS strategic communications and congressional liaison efforts and exercises his/her direction of them through his/her day-to-day oversight and management of the office's activities.

(2) Establishes NCIS strategic communications, congressional outreach, and legislative priorities and performance requirements.

(a) Communications and congressional liaison priorities respond to the Director's Strategic Vision, the priorities and performance requirements established by the Deputy Director, and the priorities and objectives of the Principal Executive Assistant Director for Management & Administration.

(b) As directed, produces for the Director's approval, a multiyear NCIS Strategic Communications Plan that guides NCIS internal and external communications.

(c) Collaborates with the program, field, and global executives, and the Planning and Evaluation Department and produces an annual "State of the NCIS" Performance Assessment Report for departmental seniors.

d. Accountable to the Director for the agency's success in meeting its strategic communications mission; responsible to the program and field executives for a public affairs program responsive to the combating terrorism, counterintelligence, and criminal investigative missions.

e. Roles and Responsibilities of the Communications Director

(1) Serves as the Director's principal advisor regarding strategic communications and congressional liaison.

(2) Provides leadership for the activities of the NCIS Office of Communications.

(a) Directs the development of NCIS strategic communications, congressional .outreach, and legislative priorities and performance requirements.

(b) At higher direction, produces the multiyear NCIS Strategic Communications Plan that guides its internal and external communications outreach and the design, development, procurement, and operation of NCIS communications tools, venues, and products.

(3) Supervises, reviews, and evaluates Deputy Communications Director performance.

(4) Oversees and manages the office's day-to-day activities, specifically,

(a) Congressional Outreach and Liaison

1. Coordinates education and subject matter briefings for Members of Congress and their staffs.

2. Research and produce information papers and briefing materials for Members of Congress, congressional committees/subcommittees, and staffs as required.

3. Produce annual budget/mission accomplishment briefs for congressional oversight bodies.

4. Research and produce agency responses to congressional inquiries.

5. Prepare and pursue enactment of legislation that would enhance the ability of NCIS to accomplish its mission.

6. Analyze, monitor, and track legislation that could affect agency authorities or ability to accomplish its mission.

7. Manage NCIS participation in the Navy Legislative Fellows program.

(b) Stakeholder and External Communications. Promote awareness of the NCIS mission and accomplishments among stakeholders, particularly among the departmental leadership.

1. Produce the Secretary of the Navy weekly NCIS report ("NCIS News to You".)

2. Produce articles and features for Navy Chief of Information products, e.g. "Day in the Navy, "Rhumb Lines," and All Hand's.

3. Collaborate with the Planning and Evaluation Department and produce the annual "Year in Review" report highlighting organizational achievement.

4. Collaborate with the program, and the three field directorates executives, and the Planning and Evaluation Department and produce an annual "State of the NCIS" Performance Assessment Report.

(c) Monitor, track, and analyze media interests relative to NCIS; produce timely and accurate information products/media inquiry responses related to the agency's composition, mission, and specific activities that promote NCIS interests.

1. Coordinate media inquiry responses with stakeholder and partner agencies as required.

2. Manage NCIS national media outreach efforts and media access to NCIS; oversee liaison with CBS/Paramount.

3. Coordinate publicity and entertainment-related events with studio, producers, and actors; facilitate technical support to writers; and coordinate memorabilia-related requirements.

4. Manage the "NCIS Brand" and its implementation.

5. Manage the external (public-facing) NCIS website, its content, and responses to website-generated inquiries.

6. Produce and maintain the NCIS Mission Brief for agency use.

7. Provide photographic and videography support in the National Capital Region and elsewhere as circumstances permit and organization-wide graphic arts support.

(d) Internal Communications

1. Support the Director and executive staff internal strategic communications efforts; as required, produce information products in support of internal strategic communications.

2. Publish the NCIS "Bulletin and Bulletin Spotlight."

3. Produce the Director's podcast, special event general administrative documents, "Death in the NCIS Family" general administrative documents, and social media-related products, as required.

4. Provide graphic arts and video graph support to organizational events and operational programs.

(e) Liaison Activity and Event Management and Support

1. Manage NCIS' participation in events and conferences sponsored by national and international law enforcement organizations, including the International Association of Chiefs of Police, Women in Federal Law Enforcement, Hispanic American Police Command Officers Association, National Organization of Black Law Enforcement Executives, and National Asian Peace Officers' Association.

2. Manage NCIS Director-sponsored liaison events, including the Director's Holiday Liaison Event and the annual Liaison Officers' Association Event.

3. Coordinate and/or support NCIS Headquarters-sponsored ceremonial events and meetings, e.g., award/retirement ceremonies, heritage events, and liaison outreach meetings.

4. Manage NCIS headquarters liaison Emergency and Extraordinary Expense and bulk memento requirements.

2-25. Inspector General

a. Serves as the principal advisor to the Director for issues regarding the efficiency, effectiveness, and integrity of NCIS activities and personnel; serves additional duty on the staff of the Naval Inspector General.

b. Directs the activities conducted by NCIS to plan, implement, and maintain activities to ensure agency compliance with U.S., DoD, DON, and NCIS standards, rules, and regulations and to promote the integrity and professional responsibility of the NCIS workforce.

(1) Exercises leadership of NCIS component performance evaluation, regulatory compliance, and personnel integrity efforts and exercises his/her direction of it through his/her day-to-day oversight and management of the office's activities.

(2) Establishes NCIS inspection and compliance oversight policy, guidance, priorities and performance requirements.

c. Accountable to the Director for the agency's component performance evaluation, regulatory compliance, and personnel integrity/professional responsibility oversight mission; responsible to the program and field executives for a transparent performance/compliance evaluation process which identifies, resolves, and shares findings and issues (including "best practices") of value and a professional responsibility review process which promptly and thoroughly investigates and resolves allegations of employee misconduct.

d. Roles and Responsibilities of the Inspector General

(1) Serves as the Director's principal advisor regarding NCIS component performance evaluation, regulatory compliance, and personnel integrity/professional responsibility oversight.

(2) Serves as the primary NCIS point of contact within the Inspector General community; serves as the Director's representative to the Defense Council on Integrity and Efficiency.

(3) Directs the NCIS Inspection Programs

(a) Formal NCIS Inspector General Inspections

1. Establishes, publishes, and revises as necessary the triennial NCIS Headquarters Inspection schedule.

2. Establishes and produces, in conjunction with the Management & Administration Directorate, policy guidance and program standards.

3. Executes the program through his supervision of the Headquarters Inspection Team Leaders.

(b) NCIS Self Inspections and Assessments

1. Establishes and produces, in conjunction with the Management & Administration Directorate, policy guidance and program standards to assist program, and the three field directorates executive implementation of program requirements.

2. Reviews and evaluates self-inspection assessments; recommends corrective action as required.

(c) Semi-Annual Management Visits

1. Establishes and produces, in conjunction with the Management & Administration Directorate, policy guidance and program standards to assist the three field directorates implementation of program requirements.

2. Reviews and evaluates management visit reporting; recommends corrective action, and shares information of value as warranted.

(4) Manages the NCIS Intelligence Oversight Program.

(5) Manages the NCIS Managers' Internal Control Program. Produces the NCIS statement of assurance for the Director's approval and release.

(6) Serves as the independent auditor of the NCIS headquarters Emergency and Extraordinary Expense fund.

(7) Advises the Director, Deputy Director, and Principal Executive Assistant Director on personnel and personnel-related decisions including, but not limited to:

(a) Promotions, transfers, and awards nominations.

(b) Issuance of non-police badges.

(c) Issuance of firearms authorization and firearms to non-agent personnel.

(8) Provides leadership for the activities of the NCIS Office of Inspections. Directs the development of NCIS inspection, compliance oversight, and employee misconduct investigative priorities and performance requirements.

(9) Supervises, reviews, and evaluates the Deputy Inspector General performance.

(10) Oversees and manages the office's day-to-day activities. Executes through direction to, and supervision of, the Deputy Inspector General.

(a) NCIS Inspector General Investigations. Ensures that NCIS Inspector General-conducted and directed investigations (category 2B), inquiries (category 2C), and DON Hotline Complaint investigations are conducted, concluded, and reported in a timely and thorough manner.

(b) NCIS Inspection Program

1. Ensures that formal NCIS inspections are scheduled, conducted, and concluded in a timely and thorough manner; prepare and publish inspection reports which include, when necessary, actionable findings and recommendations and, when appropriate, "best business practices" for consumption by other field elements.

2. Directs the program, and the three field directorates executives to perform annual self-inspection assessments within their spheres of responsibility and to perform and oversee their field office management visits.

3. Reviews and evaluates self-inspection assessment and management visit reporting; recommends corrective action/shares information of value as warranted.

(11) Engages executive-level communications, internally and externally, in order to advise, inform, and influence NCIS employees, customers, stakeholders, and partners.

(a) Keeps the Director, Deputy Director, the Principal Executive Assistant Director, and NCIS executives informed on all matters pertaining to NCIS component performance evaluation, regulatory compliance, and personnel integrity.

(b) Articulates NCIS, Director, Deputy Director, and Principal Executive Assistant Director policy positions and equities,

(c) Educates and influences stakeholders, resource sponsors, and liaison partners.

(d) Shares information of value.

2-26. NCIS Counsel (Detailed), Office of the General Counsel of the Navy

a. Appointed by the General Counsel of the Navy to serve as the principal advisor to the NCIS Director and his/her staff for legal advice and counsel.

b. Accountable to the Navy General Counsel for providing the NCIS with legal solutions for its operational, business, and other challenges and needs; responsible to the Director, the Deputy Director, program, and the three field directorates (Atlantic, Pacific and Global Operations) executives for legal advice and counsel, effective advocacy, and creative problem solving responsive to, and supportive of, NCIS' combating terrorism, counterintelligence, criminal investigative, and administrative missions.

c. Roles and Responsibilities of the NCIS Counsel

(1) Serves as the principal legal advisor for the Director and the NCIS executive staff.

(2) Provides leadership for the activities of the NCIS Legal Office. Establishes NCIS legal office priorities and performance requirements.

(3) Manages the NCIS Ethics, Oral, Wire/Electronic Intercept, and Freedom of Information, and the Privacy Act Programs.

(4) Supervises, reviews, and evaluates legal office personnel performance.

(5) Oversees and manages the office's programs and day-to-day activities, specifically:

(a) Legal counsel and advice to senior managers regarding NCIS operations, investigations, and other operational activities including, but not limited to:

1. Search and seizures, physical and in cyberspace.

2. Criminal procedure and Uniform Code of Military Justice procedure.

(b) Legal counsel and advice to senior managers regarding NCIS administration and management activities including, but not limited to:

1. Employee disciplinary investigations and administrative actions.

2. Processing discrimination and reprisal complaints.

3. Protecting personally identifiable information (PII) and PII information sharing.

4. Military personnel and military justice matters.

5. Government ethics, conflicts of interests, and post-Government employment restrictions

(c) Formal legal review of proposed/on-going operational activities including, but not limited to:

1. Sensitive intelligence and intelligence-related activities.

2. Intelligence-related procedures for collecting information on U.S. persons.

3. Draft National Security Letters for use in counterintelligence, and counterterrorism investigations.

4. Requests for oral, wire, and/or electronic intercepts.

5. NCIS conflict of interest investigations

6. Make required notification to Office of Government Ethics.

(d) Formal legal review of NCIS responses to external tasking, draft policies and manual chapters, and memoranda of understanding or agreement.

(e) Legal and sufficiency reviews of NCIS vehicle mishap reports and resulting JAG Manual investigations.

(f) Represent or facilitate and support other representation of NCIS and its personnel during litigation including, but not limited to:

1. Administrative litigation before the Merit Systems Protection Board and Equal Employment Opportunity Commission resulting from disciplinary actions, discrimination complaints, and reprisal complaints.

2. Obtain and support Department of Justice (DOJ) representation in civil litigation against NCIS employees for incidents arising within the scope of official duties.

3. Support DOJ efforts in civil litigation in which the DoD or DON is a party and in which NCIS has an interest.

4. Support discovery and discovery-related requests emanating from civilian criminal court and military courts-martial litigation.

(g) Freedom of Information/Privacy Act Request Processing

1. Receive and process requests for compliance.

2. Locate records responsive to requests.

3. Obtain classification review of classified responses.

4. Process responsive records using statutory criteria.

5. Provide processed records to requestor within statutory time limits.

(6) Engages executive-level communications, internally and externally, in order to advise, inform, and influence NCIS employees, customers, stakeholders, and partners.

(a) Keeps the Director, Deputy Director, the Principal Executive Assistant Director, and NCIS executives informed on all legal issues and matters of interest.

(b) Articulates NCIS, Director, Deputy Director, and Principal Executive Assistant Director policies, positions and equities.

(c) Produces monthly “Legal Briefs” highlighting significant and relevant developments in law and providing practical guidance to NCIS personnel.

(d) Shares information of value.

2-27. Chief Diversity Officer/Deputy Equal Employment Opportunity Officer

a. Serves as the principal advisor to the Director for issues regarding NCIS workforce diversity and equal employment opportunity.

b. Directs the activities conducted by NCIS to plan, implement, and establish a workforce which reflects our national diversity and ensures equal opportunity for all NCIS employees; responsible for establishing and maintaining a culturally diverse NCIS workforce and a workplace culture which respects the dignity, contributions, and advancement opportunities of all employees.

(1) Exercises leadership of NCIS workforce diversity development and equal opportunity efforts and exercises his/her direction of it through his/her day-to-day oversight and management of the Diversity Management Office's activities, the activities of the Diversity Advisory Committee, and through his/her collaboration with the Assistant Director for Human Resources.

(2) Establishes NCIS workforce diversity and equal opportunity priorities and performance requirements.

(a) Workforce diversity and equal opportunity priorities respond to the Director's Strategic Vision and the priorities and performance requirements established by the Deputy Director.

(b) As directed, produces for the Director, an annual NCIS Diversity Recruitment Plan that guides NCIS diversity recruitment efforts and informs the Human Resources Directorate's overarching agency recruitment strategy.

c. Accountable to the Director for the Agency's success in meeting its workforce diversity and equal opportunity mission; responsible to the program and the three field directorates executives for diversity and equal opportunity programs that are responsive to, and supportive of, the combating terrorism, counterintelligence, and criminal investigative missions.

d. Roles and Responsibilities of the Diversity Officer/Deputy Equal Employment Opportunity Officer

(1) Serves as the Director's principal advisor regarding workforce diversity and equal employment opportunity.

(2) Provides leadership for the activities of the NCIS Office of Diversity Management and Equal Employment Opportunity and the NCIS Diversity Advisory Committee.

(a) Directs the development of NCIS workforce diversity and equal opportunity priorities and performance requirements.

(b) At higher direction, produces for the Director, an annual NCIS Diversity Recruitment Plan that guides NCIS diversity recruitment efforts and informs the Human Resources Directorate's agency recruitment strategy.

(3) Manages the NCIS Alternative Dispute Resolution Program.

(4) Oversees cultural awareness and equal employment opportunity awareness training.

(5) Assess NCIS field office Equal Employment Opportunity compliance as part of the NCIS Inspection Program.

(6) Oversees the NCIS discrimination complaint/investigative process.

(a) Informally resolves complaints when appropriate.

(b) Reviews discrimination complaint investigation to ensure timely completion, sufficiency of coverage, and adherence to Title VII principles.

(c) Recommends corrective action/remedies for the Director and executive staff regarding discrimination complaints.

(7) Supervises, reviews, and evaluates office personnel performance.

(8) Oversees and manages the office's day-to-day activities, specifically those of the Equal Employment Opportunity counselors/specialists:

(a) Discrimination and employment practice complaint investigations and reporting.

(b) Maintenance of the NCIS portion of the Navy Discrimination Complaint Database.

(c) Perform recurring data and barrier analyses on protected groups and areas, as required. Review Human Resources Directorate policies and procedures to ensure full accessibility and availability.

(d) Provide Equal Employment Opportunity Program support for NCIS programs, events, and initiatives.

(9) Engages executive-level communications, internally and externally, in order to advise, inform, and influence NCIS employees, customers, stakeholders, and partners.

(a) Keeps the Director, Deputy Director, the Principal Executive Assistant Director, and NCIS executives informed on all matters pertaining to workforce diversity and equal employment opportunity.

(b) Articulates NCIS, Director, Deputy Director, and Principal Executive Assistant Director policy positions and equities,

(c) Educates and influences stakeholders, resource sponsors, and liaison partners, and

(d) Shares information of value.

2-28. NCIS Comptroller

a. Serves as the chief financial advisor to the Director.

b. Directs the financial operations of the agency. Responsible for providing accounting, budget formulation; budget execution; financial management and policy; financial systems; and financial/cost reporting support for the agency.

c. Accountable to the Director for ensuring that the agency's funding is effectively, efficiently and legally executed.

d. Roles and Responsibilities of the Comptroller

(1) Serves as a senior advisor to the Director and Deputy Director in the areas of budgeting, accounting, reimbursable program management, and travel and manpower affordability.

(2) Identifies resource efficiencies and advises on opportunities for improved mission effectiveness. Develops, coordinates, integrates, and executes financial management policies, programs, and processes for the effective and efficient control and utilization of the Agency's annual budget.

(3) Ensures Agency compliance with the Chief Financial Officers Act of 1990, Government and Performance Results Act of 1993, SECNAVINST 7000.27A and subsequent legislation and regulations pertaining to financial planning and reporting.

(4) Manages a viable internal controls program to ensure compliance with all applicable laws and regulations and assist management in effectively, efficiently and economically carrying out its financial stewardship responsibilities.

(5) Ensures adequate financial resources are available for achievement of the goals and objectives of the Agency; that such resources are employed in the most effective and efficient manner, and that NCIS is in compliance with all applicable legal, regulatory, and policy requirements.

(6) Manages the organization's Debt Management program for overpayments and collection of government funds.

(7) Provides management oversight necessary for directing activities of the Comptroller's Office. Activities include development, implementation, and review of accounting programs and operations; formulation, presentation, and execution of the budget; managerial-financial reporting; financial management automated systems, personnel-payroll interface, including development, maintenance, and dissemination of all financial codes related

to personnel administration; and management advisory services for all NCIS leaders and Program Managers to improve cost effectiveness, efficiency, productivity, and to avoid loss.

(8) Engages executive-level communications, internally and externally, in order to advise, inform, and influence NCIS employees, customers, stakeholders, and partners.

(a) Keeps the Director, Deputy Director, and NCIS Executive Assistant Directors informed on all matters pertaining to financial management.

(b) Articulates NCIS, Director and Deputy Director policy positions and equities.

(c) Educates and influences stakeholders, resource sponsors, and liaison partners.

(d) Shares information of value.

NCIS-1, Chapter 3
NCIS Executive Decision Making Process
Effective Date: May 2013

Table of Contents

Reference:
(a) SECNAVINST 5430.107, Mission and Functions of the Naval Criminal Investigative Service
(b) Department of the Navy Correspondence Manual, Secretary of the Navy Manual 5216.5, March 2010

3-1. Purpose. This chapter sets forth the NCIS Ex**e**cutive Decision Making Process (EDMP) with definitive procedures for receiving, assigning, processing, tracking, monitoring, completing, documenting, and communicating executive decisions throughout NCIS.

3-2. Policy

a. The Director and the Deputy Director are recognized as the NCIS executive leadership with executive decision making authority. Policy in this chapter provides the mechanism to assist the Director and the Deputy Director in making prompt and well-informed decisions, to standardize authority and responsibility, to ensure efficiency and effectiveness, and to record and disseminate executive taskings and decisions for required staff or operational action.

b. The Director, NCIS, is authorized to organize, assign, and reassign responsibilities among NCIS subordinate activities (reference (a)). The Director, NCIS must review and sign documents that:

(1) Establish policy,

(2) Center on NCIS' mission or efficiency, and are addressed to higher authority,

(3) Deal with certain aspects of military justice, and,

(4) Are required by law or regulation.

c. The Director, NCIS, maintains Original Classification Authority (OCA) by virtue of the position for approving the designation of classified material as TOP SECRET. The Director's, OCA authority is not transferable (SECNAV M-5510.36 Department of the Navy Information Security Program applies).

d. The Deputy Director, NCIS, is responsible for the daily oversight and management of the organization and all of its activities, including those of the NCIS operational, field, and management and administrative directorates. All executive decision packages require review by the Deputy Director. The Deputy Director, NCIS, may sign an executive decision package by:

(1) title;

(2) specific delegated authorities;

(3) "By direction" authority;

(4) in his or her capacity while serving during absences of the Director, NCIS as "Acting."

e. The Chief of Staff (NCIS Code 01C (CoS)) will serve as the final formal official staff reviewer on all executive decision packages prior to review and approval by the Deputy Director and Director. The CoS will coordinate the flow of the packages within the Office of the Director, and facilitate substantive decision-related discussion with executive assistant directors (EADs), assistant directors (ADs), and the Director's immediate staff (Communications, Comptroller, Inspector General and Counsel) when necessary.

f. The CoS is the arbiter of actions requiring Director or Deputy Director approval and actions having the Director's and the Deputy Director's interest. NCIS executives and senior managers are encouraged to consult with the CoS when preparing executive decision packages to ensure proper Office of the Director awareness.

g. This chapter directs the Deputy Assistant Director (DAD) for Administrative Services, Code 11C, to provide support and to direct the flow of executive decision packages and staff actions to the NCIS executive leadership. Code 11C will coordinate his or her activities with the CoS.

3-3. Cancellation. The policy issuances identified below are cancelled.

a. Gen Admin 11C-0002 of 4 January 2011 (NCIS Policy Document No 11-01 Administrative (Interim Guidance for the NCIS Executive Decision Making Process).

b. NCIS-1, Chapter 3 - Executive Decision Making Process of June 2009.

c. NAVCRIMINSERVINST 5420.1E Official Correspondence Signature and Release Authority Policy of 30 December 2004.

d. NAVCRIMINSERVINST 5000.2C Standard Operating Procedures for the Completion of Staff Actions within Headquarters, Naval Criminal Investigative Service of 19 January 2005.

3-4. Chapter Sponsor. The chapter sponsor for this chapter is the Administrative Services Department, Code 11C.

3-5. Definitions

a. Executive Decision. An executive decision is an official documented statement that approves new or revised policy, or approves courses of action that compel headquarters or field activities to execute a new mission or task. An executive decision also includes responses to taskings from Department of the Navy (DON) or Department of Defense (DoD) leadership which explicitly requires signature from the Director or the Deputy Director.

b. Executive Tasker. An executive tasker is an action or issue that has the Director's or Deputy Director's interest, or requires an executive decision.

c. Decision Maker Interest (DMI) Item. A DMI item is any action having the immediate interest of the Director or Deputy Director. A DMI action item is flagged for special attention and expeditious processing. DMI items will be flagged on NCIS Routing Sheet NCIS 5000.8D (Revised 09/2011) (Appendix A, also referred to as the green blazer).

d. Executive Decision Package. An executive decision package presents documents for review and decision by the Director or Deputy Director.

e. NCIS Routing Sheet, NCIS 5000.8D (Rev. 09/2011). The NCIS Routing Sheet (also referred to as green blazer) documents required reviews and provides a written explanation of the executive decision making package contents, and recommends a course(s) of action. A copy of the green blazer is provided at Appendix A; the document can be downloaded from the forms tab on NCIS Lighthouse.

f. Action Memo. An action memo is a document that succinctly and concisely identifies and presents solutions or alternatives to potential or existing problems. An action memo may propose the establishment of new policy, or recommends revision to existing policy. An action memo may also include correspondence proposing, informing or responding to senior DON or DoD leadership. An action memo must comply with the requirements of reference (b). A sample action memo format is provided in Appendix B.

g. Policy. Policy is defined as organizational tenets and directives that guide how NCIS executes its mission, functions, and roles and responsibilities as defined in references (a). NCIS policy is contained in NCIS manuals, current policy documents, and NCIS instructions. Only the Director is vested with the authority to establish or modify NCIS policy.

h. Policy Change. A policy change involves any action that modifies the mission, function, or roles and responsibilities of any part of NCIS.

i. Policy Document. A policy document is any document that defines the way ahead, or outlines processes and procedures within NCIS through issuance of NCIS manuals and chapters, policy documents promulgated through General Administration SSD messages, and NCIS instructions approved by the Director.

j. Action Officer (AO). A person assigned responsibility for researching, preparing, and contributing to the completion of an executive decision package or staff action.

k. Lead Action Office. The office assigned primary responsibility for the completion of the staff action and presenting the executive decision package. The lead action office is responsible for ensuring that coordinating offices provide input to the package and that established deadlines are met. The AO representing the lead action office is the primary point of contact to Code 11C. The AO is responsible for notifying Code 11C when established deadlines cannot be met.

l. Coordination Office. The office(s) assigned responsibility to review and provide input to the executive decision package. The coordination office representative must provide feedback to Code 11C when established deadlines cannot be met.

m. Action Due (Suspense) Date. A specific date assigned to complete the task.

3-6. Items Requiring an Executive Decision. The following actions are representative of items requiring either an executive decision or which will routinely invoke Director or Deputy Director interest:

a. Policy documents and NCIS chapters.

b. Final Seat of Government, DoD, or DON tasking responses.

c. Human resources actions, specifically:

(1) Selections for SES, DISES, and DISL positions.

(2) Promotions to GS-14, GS-15, and equivalent DCIPS grades.

(3) Selections as supervisory special agents.

(4) Awards.

(5) Employee transfers.

(6) Employee requests for policy exemptions.

(7) Annuitant requests and selections.

(8) Disciplinary actions that are appealable with the Merit Systems Protection Board.

d. NCIS budget and budget related submissions requiring review, endorsement or concurrence by the Secretary or the Navy's Secretariat Offices.

e. Manpower recommendations.

f. DON action and information memorandums.

g. Operational information memorandums.

h. Request for forces recommendations and assignment selections.

3-7. Responsibilities

a. EADs, Chiefs, and ADs must monitor their directorates and field activities to facilitate the smooth flow of documents required by the Director or Deputy Director. EADs, Chiefs, and ADs, are responsible for reviewing and recording their directorate level review chop (concur or non-concur) on all executive decision packages submitted for an executive decision and are personally accountable to the Deputy Director for their directorate positions.

b. DADs must work closely with their departments to facilitate the smooth flow of documents required by EADs, Chiefs, or ADs to support the Director or Deputy Director in making executive decisions. DADs will be responsible to review and record their review, and obtain the required directorate level review on executive decision packages prior to submission to Code 11C. These leaders will also:

(1) When assigned as the lead action office, assign an AO to produce the executive decision package, as directed. Ensure AOs and coordination office complete assigned staff actions according to prescribed formats and within assigned deadlines.

(2) When assigned responsibility as a coordination office, ensure timely, accurate, and complete information is provided to the lead action office AO.

(3) Conduct a quality review to ensure timeliness, accuracy, and completeness of executive decision packages.

c. Code 11C will serve as the central collection point and cross-functional facilitator for all issues requiring an executive decision and all executive taskers. Specifically, Code 11C will:

(1) Establish deadlines, and coordinate and monitor all actions requiring executive decision to ensure completion.

(2) Coordinate with the CoS to determine which external and internal taskers must be identified as DMI items. Code 11C will annotate those actions deemed to be DMI items in the Tasker System tracking tool.

(3) Review packages submitted to the Director or Deputy Director for completeness to include, but not limited to, ensuring that applicable references and supporting documents are included in the package. Code 11C will also assist the lead action office by monitoring coordinating offices, both internal and external, to review compliance with established deadlines.

(4) Coordinate with the CoS to receive requests for follow-up actions required by the Director or Deputy Director to finalize decisions, and relay, when requested, the requirements to the appropriate codes.

(5) Return approved executive decision packages to the appropriate codes for required action.

(6) Track the status of implementing actions approved by the Director or Deputy Director.

(7) Maintain the central archive for all executive decision packages.

d. Lead Action Office. Develop, coordinate and complete required analysis, formulate recommendations, present issues for executive decision, and prepare necessary correspondence implementing recommendations. The lead action office AO should provide alternative options, evaluations of each option, and provide recommendations. The lead action office AO must also ensure executive decision packages are coordinated with the appropriate NCIS directorates, departments or field offices. The lead action office AO is also responsible to coordinate with the appropriate DoD, and DON offices when required.

3-8. Executive Decision Process. There are several sources from which staff actions enter the decision making process. In each case, a determination must be made as to whether the staff action requires an executive decision and thereafter whether it must be designated as a DMI item.

a. Taskings received from external sources:

(1) Code 11C receives the majority of tasks from external sources such as the Office of the Secretary of Defense, the Secretary of the Navy staff, and the Service staffs. There may be tasks from other Seat of Government agencies that also fall into this category.

(2) Upon receipt, Code 11C will analyze whether the item will require an executive decision. If such identification is not clear, Code 11C will consult with the CoS, EADs, Chiefs, and ADs, in making a proper determination. All external items requiring an executive decision will automatically be annotated as a DMI item.

(3) There are occasions when NCIS Headquarters directorates and departments receive taskings directly from an external source. When these taskings have the potential to impact or change existing NCIS roles, responsibilities and authorities, or internal NCIS policies, processes and procedures, the response requires the Director's or Deputy Director's decision or signature. Accordingly, when departments receive external taskings directly, they will provide a copy to Code 11C for central processing and tracking.

b. Taskers Generated by the Director or Deputy Director

(1) Taskers generated by the executive leadership come from a variety of sources. Those captured in official correspondence typically assign responsibilities for each tasking and are relatively easy to identify.

(2) However, many taskings and decisions come from less structured sources to include staff meetings, briefings, conferences, and command visits. Generally, EADs, Chiefs, or ADs attending such forums understand the tasking or decision and begin appropriate action. The challenge in these instances is to capture the specific tasking or decision, the office code(s) assigned responsibility for the action, and any established deadlines.

(3) In order to capture these taskings, the CoS will identify the appropriate DMI taskings from the various sources to Code 11C. Code 11C will establish action deadlines, enter the item into the Tasker System, and notify the appropriate lead action office.

(4) Code 11C will also coordinate with the CoS, EADs, Chiefs, or ADs to identify those items that will require an executive decision and those that must be flagged as DMI items in the Tasker System.

c. Proposals or recommendations generated internally by NCIS headquarters directorates, departments, or field activities that require an executive decision, or warrant being marked as a DMI item, must also be identified. DMIs nominated by directorates, departments or field activities must be coordinated through 11C.

(1) Generally, directorates or field activities will present such proposals or recommendations in writing using an executive decision making package.

(2) Similarly, in those cases where the Director or Deputy Director makes a decision as a result of briefings provided to them, a record of the decision must be captured. In those cases, the applicable directorate will prepare an executive decision package for the Director or Deputy Director's review or signature. These packages will capture the background and rationale for the decision. Documents included in the executive decision package will be retained as the official record of the decision. The executive decision package will be archived by Code 11.

(3) The executive decision package must include all documents needed for the decision maker to effect a decision or sign correspondence. The executive decision package must include:

(a) The NCIS Routing Sheet NCIS 5000.8D (green blazer). Block number 13 of the green blazer must include a succinct and concise written statement so that the Director or Deputy Director can read what is included in the package; the purpose of the documents contained in the executive decision package, and recommended course(s) of action relevant to the issue(s) being presented. If additional information is needed to complete block number 13, the AO can continue on a second page using plain white paper, or

(b) Include a succinct and concisely written action memo so that the Director or Deputy Director can read what is included in the package, the purpose of the documents contained in the executive decision package, and a recommended course(s) of action relevant to the issue(s) being presented. If an action memo is used, the AO must annotate the green blazer, block number 13 as "see attached action memo."

d. Code 11C will enter items for an executive decision or items flagged as a DMI item into the Taskers System tracking tool to facilitate monitoring of tasks through completion. Each task item will identify all pertinent information to include lead action and coordination responsibilities, suspense dates, and deliverables. The lead action office is responsible for consolidating inputs from the other coordinating codes, and preparing or providing required correspondence and, or other supporting reference documents.

e. The lead action office assigned to coordinate the executive staff action will prepare the executive decision package. This includes preparing the green blazer which must be attached electronically to the final staffing package after the lead action office completes necessary research and staffed the package through the appropriate EADs, Chiefs, ADs, and DADs. The lead action office AO will also prepare any correspondence requiring signature.

f. Executive decision packages must have the endorsement of the appropriate EAD, Chief, AD, and DAD prior to being routed to Code 11C. After receiving EAD, Chiefs or AD endorsement, all packages requiring review and signature by the Director or Deputy Director will be forwarded electronically to Code 11C. Hard copy references and supporting documents may be provided if electronic copies are unavailable.

g. All executive decision packages must be coordinated and processed to the Director or Deputy Director through Code 11C. Executive decision packages must not be hand-carried directly to the Director or Deputy Director. Staffing of these packages through Code 11C allows for proper tracking, and ensures that required follow-up or additional information is provided to the executive decision-makers. Processing executive decision packages through Code 11C also ensures that actions approved by the executive decision-makers are recorded and promulgated to the organization.

h. Once the executive decision package is received from the lead action office AO, Code 11C will route the package for NCIS Counsel review prior to submitting the decision package to the CoS. The CoS in coordination with Code 11C will identify those executive decision packages requiring coordination review by the Inspector General.

3.9. Concurrence – Non-Concurrence

a. Coordinating directorates or departments will indicate concurrence or non-concurrence on the NCIS green blazer. Coordinating codes are expected to provide concurrence or non-concurrence in a timely manner.

b. Non-concurrence requires approval by the EAD or Chief and must be accompanied by specific objections and supporting rationale. Concerns or recommended changes to the

executive decision package that do not meet the level of non-concurrence, but are of such substantive change to warrant discussion, must be included in the package.

(1) If a directorate, department, or field office non-concurs with an executive decision package, the package will be returned to the lead action office AO for resolution prior to presentation to the Director or Deputy Director. Attempts to resolve conflicting opinions must take place first at the department level. If a disagreement cannot be resolved at the department level, the issues must be raised to the EADs or Chiefs for resolution. EADs and Chiefs should make every attempt to resolve disagreements prior to presenting the executive decision package to the Deputy Director for an executive decision.

(2) Issues requiring the Director or Deputy Director approval and having their interest which cannot be resolved at the EAD or Chief level will be arbitrated by the CoS.

c. Once the executive decision package is approved by the Director or Deputy Director, it will be returned to Code 11C. The package will be delivered to the intended recipient, with a copy going to the originating or lead action office and the official copy being archived by Code 11C.

d. Code 11C will work with the originator or lead action office AO to coordinate the method by which the executive decision package will be promulgated, and to what audience.

3-10. Timelines. Code 11C is chartered to coordinate staffing of all policy actions and documents, external and official internal tasking, tasking received by other program elements from external customers for tracking and proper routing. As such, Code 11C will closely monitor taskers, actions, and overdue and outstanding correspondence in an effort to ensure timely responsiveness to external taskers and timely decisions on internal taskings and initiatives.

a. Change to Lead Action Assignment. To appeal a lead action office assignment, the AO must contact Code 11C within 24 hours of the date of receipt with a reasonable rationale for reassignment. Code 11C, will typically accept the action for transfer without further coordination and re-task the action.

b. Action Suspense Assignment. Code 11C is responsible to assign action suspense dates based on guidance provided the CoS or as directed by SECNAV and DoD external tasks. Executive decision packages will be staffed and presented for approval within the identified deadline established by Code 11C. Review and comment deadlines that are not met without previous consultation with Code 11C will be identified to the CoS. The lead action office is responsible to contact Code 11C within 24 hours of the date of receipt of the assignment to request an extension with a reasonable rationale for the extension.

(1) Code 11C will contact the external tasking office to request an extension using the rationale provided by the lead action office AO.

(2) A request for extension by the external tasking authority may or may not be accepted by the appropriate tasking authorities. In some instances, Code 11C may successfully negotiate a date meeting the requirements of both parties.

c. Congressional Correspondence. Special attention must be given to congressional correspondence requiring the Director's decision or signature, or signature by Secretary of the Navy.

(1) Congressional inquiries will be answered within five working days, or by the specified due date assigned by the Secretary of the Navy's White House Liaison/Close Hold Office. Accordingly, this type of correspondence requires timely focus and attention from the assigned lead action office. Due to the seniority of the originator, the lead action office AO must pay particular attention to established deadlines assigned to congressional inquiries.

(2) If a response cannot be provided within five days, the lead action office AO must send an interim response that acknowledges receipt of the congressional correspondence and provide an estimated date when a final response will be sent.

d. "STOPLIGHT" DON Congressional Inquiry. An interim and the final response to a "STOPLIGHT" DON congressional tasker must be staffed through the Secretary of the Navy's White House Liaison/Close Hold Office prior to signature by the Director or the Secretary of the Navy.

e. Internally Generated Executive Decision Making Packages. The lead action office AO is responsible to submit internal self-generated executive decision packages to Code 11C for processing and identify a desired processing action suspense date (this does not apply to NCIS manuals and chapters). Executive staff action packages requiring a decision or signature by the Director or Deputy Director with a desired suspense date less than five-working days must include a statement in the green blazer or action memo explaining the "urgency of the package" and why the package could not be submitted with more processing lead time.

f. Code 11C will provide the Deputy Director with a monthly NCIS Staff Action Status Report. The status report will contain open and overdue staff actions. DMI staff actions will be highlighted. The status report will serve as tool for monitoring the status of DMI items and taskers, reduce and eliminate overdue taskers and forecast the status of upcoming Stoplight/DMI taskers.

3-11. Signature Authority

a. The Director, NCIS signature authority is stated in Section 3.2, paragraphs b. and c.

b. The Deputy Director, NCIS signature authority is stated in Section 3.2, paragraph d.

c. Headquarters EADs, Chiefs, ADs, and Director's immediate staff may sign official correspondence only to the extent necessary to accomplish effective management of their areas of responsibility and which does not call for the signature of the Director or Deputy Director.

d. EADs for Atlantic and Pacific Operations, Global Operations, and special agents in charge may sign correspondence and release general administrative documents, and naval messages

needed to accomplish investigative and operational matters, and intelligence reporting, within their area of operations and responsibility.

e. The Counsel to the Director may sign correspondence relating to Freedom of Information Act matters.

f. "By direction" Signature Authority. "By direction" signature authority within NCIS programs is not authorized without specific approval, in writing, from the Director, NCIS.

(1) "By direction" signature authority is granted to the CoS to sign executive correspondence in its final form "for" the Director when the Director and Deputy Director are absent and delay would fail to meet a crucial deadline.

(2) In instances where programs believe "By direction" authority is required to perform assigned roles and responsibilities, an executive decision package must be submitted to the Director via the Deputy Director. The package must include the rationale for the authority and include the signature authority letter for the Director's signature authorizing "By direction" authority. The executive decision package must be routed through Code 11C for staffing as required by this chapter.

3-12. NCIS Letterhead. NCIS letterhead format must comply with reference (b). Letterhead stationery must bear a one inch diameter seal of the DoD. This applies to all NCISHQ and field offices. A copy of the NCIS official letterhead stationery is provided at Appendix B. No other letterhead format is authorized for NCIS official correspondence. NCIS letterhead is available to download from NCIS Lighthouse forms page.

Appendix A - Routing Blazer NCIS 5000.8D (Rev 09/2011)

1. CLASSIFICATION: UNCLASSIFIED					**2. EXECUTIVE DECISION MAKER INTEREST ITEM:** *(Enter "Yes" if Applicable)*	
3. PRIORITY: ***(Check One)***					**4. DUE DATE:**	
5. TASKER NUMBER:		**6. EXTERNAL TASKER NUMBER:**			**7. UPON SIGNATURE OR DECISION RETURN TO:**	
8. ROUTING CODE: *Insert Routing Code Where Applicable*					**9.**	
A	ACTION				**SUBJECT:**	
C	CHOP					
D	DECISION					
I	INFORMATION					
O	ORIGINATOR					
S	SIGNATURE					
	10. ADDRESSEES		**11. DATE** IN	**11. DATE** OUT	**12. INITIALS** CONC	**12. INITIALS** NON
	DIRECTOR	00				
	EA TO DIRECTOR	00X				
	DEPUTY	01				
	EA TO DEPUTY DIRECTOR	01X				
	CHIEF OF STAFF	01C				
	SENIOR ADVISOR	01CX				
	LEAD STAFF	01CC				
	PRINCIPAL, EAD	01A				
	EA TO	01AX				
	DAD ADMIN	11C				
	CENTRAL ADMIN	11C2				
	COUNSEL	00L				
	INSPECTOR	00I				

13. REMARKS:

(If additional space is necessary, attach plain white paper)

Use this section to provide brief synposis describing the package. If the package contains a Decision Memo then only identify the purpose and do not restate what is already included in the Decision Memo.

1. PURPOSE:

2. BACKGROUND:

3. DISCUSSION: [Note: Refer to Section 3.8, paragraph c, subparagraphs (1) through (3) for additional guidance.

When an action memo to the Director or Deputy Director is included in the executive decision package annotate this section with the following text:

"As stated in the enclosed action memo."]

4. RECOMMENDATION: The Director [Deputy Director] sign [or approve] TAB XXX.

14. ORIGINATOR/ACTION OFFICER *(Name, Office Code, Telephone)*	**15. Code 11C Representative** *(Name, Office Code, Telephone)*
16. CLASSIFICATION: UNCLASSIFIED	

NCIS 5000.8D (Revised 09/2011) (Previous Editions are Obsolete)

Appendix B - Action Memo Format Example

The asterisks (*) indicates the number line spaces.

DEPARTMENT OF THE NAVY
HEADQUARTERS
NAVAL CRIMINAL INVESTIGATIVE SERVICE
27130 TELEGRAPH ROAD
QUANTICO VA 22134-2253

*

[Month, Day, Year]

ACTION MEMO *

*

*

FOR: DIRECTOR, NAVAL CRIMINAL INVESTIGATIVE SERVICE [UPPER CASE]
*

FROM: S. J. Author, Executive Assistant Director, Directorate Title [Use Title Case]
*
*

SUBJECT: Example of an Action Memo Format [Use Title Case]
*

- State the facts and or the action. Describe the topic of the decision. Provide brief background. A decision paper is a document, which succinctly identifies a new or revised course of action, and presents solutions or alternatives to potential or existing problems. A decision paper presents new or proposes revision to existing policy; the decision paper may also be correspondence proposing, informing or responding to senior naval leadership or leadership of the Department of Defense.

*

- Limit the action memo to one page. Provide additional information as TABs attached to the action memo.

*

- Another example – A copy of the policy document supporting this recommendation is provided at TAB A. Mention TABs (if any, or those included as part of the action memo).

*

RECOMMENDATION: Director approves recommendations identified in TAB A.
Approve_____ Disapprove _____
*

COORDINATION: Annotated on Green Blazer [or cite appropriate TAB] or NONE.
*

ATTACHMENTS:
As stated
*
*

Prepared by: Name of the Action Officer, Office Code, Phone Number, E-mail.

Ensure Classification is listed center top and bottom of page as shown

CHAPTER 4
TITLE: WORKER'S COMPENSATION
POC: CODE 10A2
DATE: MAY 08

4-1. GENERAL

a. This chapter states the authority and policy for providing compensation and benefits to Naval Criminal Investigative Service (NCIS) employees who sustain a traumatic injury, or, occupational illness, or, condition while in the performance of duty. This chapter complies with all governing laws and regulations, which for reference purposes may be found at Title 5, United States Code, Sections Title 5, United States Code, Section 8101 et seq and Title 20, Code of Federal Regulations (CFR). Detailed information on the Federal Employees' Compensation Act (FECA) may be found at the Department of Labor, Office of Workers' Compensation Programs (OWCP) Home Page.

b. The definitions applicable to this chapter are those found in the above referenced documents.

c. The benefits provided by FECA through the OWCP constitute the exclusive remedy for work related injuries or deaths.

4-2. RESPONSIBILITIES

a. The Secretariat/Headquarters Human Resources Office (S/HHRO) is responsible for administering the Workers' Compensation Program for NCIS. NCIS Personnel Operations and Services Department, Code 10A, is the point of contact for all workers' compensation issues.

b. The employee is responsible for immediately notifying their supervisor, or ensure notification is effected, in the event of a job-related injury or illness. Detailed information for the employee is available in the OWCP Pamphlet CA-11.

c. The supervisor is responsible for reviewing the circumstances of a job-related injury or illness, providing the employee with the appropriate forms, ensuring the employee obtains required medical examination and/or treatment, and submitting timely information to Code 10A.

4-3. PROCEDURES

a. If a job-related injury occurs, the employee is required to provide notice to his/her supervisor. The appropriate procedure for notification is the submission of OWCP Form CA-1. Form CA-1 may be submitted by the employee or by someone designated to act on the employee's behalf. Form CA-1 should be submitted within 30 days after the occurrence of the injury.

b. Form CA-1 is used by the employee to give notice that an injury occurred and also to request compensation under FECA. Instructions for completing Form CA-1 may be found on the above referenced website.

c. If the injury will preclude the employee's immediate return to work, the employee, to the extent practicable, should obtain from the medical authorities the earliest probable date of return to duty. Interim status reports, as appropriate, should be provided through use of OWCP Form CA-17, Duty Status Report. In the event the temporary disability continues beyond 45 days or, if it is established that a permanent total disability exists, Form CA-7, Claim for Compensation must be filed no later than 5 days prior to the expiration of the 45 day continuation of pay (COP).

d. Upon being notified an employee sustained a job related injury, the supervisor should provide the employee with Form CA-1. When the employee returns the partially completed Form CA-1, the supervisor must complete blocks 17 through 38 on the reverse side of the form and provide the employee with the Receipt of Notice of Injury.

e. If the supervisor plans to controvert the employee's claim, he/she should so advise the employee (see paragraph 4-4 for additional information). If, in conjunction with such action, compensation will be terminated (i.e., COP denied), the employee is to be provided with the information used as the basis of this action.

f. As soon as reasonably possible following an injury to a NCIS employee, the supervisor should notify Code 10A via e-mail or telephone stating the date and nature of the occurrence and the status of Form CA-1. Form CA-1 must be forwarded to OWCP within 10 working days following receipt at Code 10A of the form from the employee. The original Form CA-1 should be sent directly to Code 10A, via the appropriate field office or headquarters code. Each office should retain copies of all submitted forms. All additional information or documentation should be attached, including any information supporting a decision to controvert an injury claim. Code 10A will review each claim and forward the necessary information to the S/HHRO.

4-4. CONTROVERTING A CLAIM

The supervisor has significant responsibilities upon being notified that a job-related injury has occurred. If the employee furnishes information, or the supervisor, through investigation, develops information that in any way makes the employee's claim questionable, there is a requirement to document the discrepancy. There are several specific reasons for controverting a claim and under those circumstances COP may not be approved. Those circumstances are as follows:

a. If the disability is a result of an occupational disease or illness; and/or,

b. If the employee is neither a citizen nor a resident of the United States or Canada; and/or,

c. If the injury occurred off the employing agency's premises and the employee was not performing official duties; and/or,

d. If the injury was caused by the employee's willful misconduct, the employee intended to bring about the injury or death of himself or another person, or, the employee's intoxication or illegal drug use was the proximate cause of the injury; and/or,

e. If the injury was not reported on form CA-1 within 30 days following the injury; and/or,

f. If the work stoppage first occurred more than 90 days after the injury; and/or,

g. If the employee initially reports the injury after his/her employment has terminated.

4-5. TEMPORARY LIMITED OR LIGHT DUTY ASSIGNMENTS

a. Department of the Navy policy mandates that employees temporarily unable to perform the full duties of their job because of medical restrictions due to work related injuries shall, to the maximum practical extent, be placed on limited/light duty with less demanding physical requirements. Ordinarily, it is expected that a partially recovered employee will eventually recover in full. In the event that an employee is eligible for temporary limited/light duty assignments the employee and the supervisor have certain responsibilities.

(1) The employee must provide documentation from a physician stating any physical restrictions, including prognosis/diagnosis and approximate duration of the medically advised restriction. The employee must immediately notify their supervisors, in writing, when he/she is able to return to work and/or to full capacity.

(2) The supervisor must ensure that limited/light duty, either within or outside the usual work area, is provided to an employee with occupational injuries/illnesses. If medical restrictions are extended beyond 30 days, the supervisor must ensure that updated medical documentation has been obtained to determine the length of limited/light duty. If it becomes apparent that an employee is permanently injured as a result of on-the-job injuries, Code 10A in conjunction with S/HHRO, should be consulted about the permanent placement programs for occupationally injured employees, or the reemployment procedures for separated employees on OWCP periodic rolls.

4-6. RECURRENCE OF DISABILITY

In the event an employee suffers a recurrence of a disability linked to a previous injury and this status results in additional work stoppage, certain actions must be taken.

a. If the employee's initial claim was approved by OWCP and he/she suffers a recurrence of disability and stops work, the employee must complete Form CA-2a. The employee must advise the supervisor whether he/she wishes to continue to receive regular pay or change the absence to sick or

annual leave. The supervisor must promptly complete part B of the form and submit to Code 10A.

b. If the recurrence takes place within 45 days of the date the employee first returned to work following the initial disability, the employee may elect to again utilize COP provided the 45 calendar days were not all "used" during the initial period of disability.

c. If the 45-day entitlement period for continuation of pay has been exhausted or 45 days have elapsed since the employee first returned to work, COP does not pertain. OWCP will be responsible for initiating payment of compensation. To obtain compensation, the employee must file a claim for any wage loss on the appropriate Form CA-7.

d. If the recurrence of disability takes place after the passage of 90 days, authorization for further medical care must be obtained from the OWCP.

4-7. SUBMISSION AND COORDINATION OF CLAIMS

All NCIS offices shall, at a minimum, keep a supply on hand of the following Forms: CA-1, CA-2, CA-7, CA-17, CA-20, and CA-1500. In the event of a job-related injury, the supervisor will ensure the appropriate form is completed and sent to the respective field office or headquarters code for further processing. The field office or headquarters code is then responsible for forwarding the claims directly to Code 10A. In the event an injury of a non-disabling nature occurs while the employee is TDY, Form CA-1 will be completed by the closest appropriate supervisor, and, in turn, forwarded to the field office or headquarters code of the employee concerned. Subsequent bills should be submitted directly to OWCP via Form CA-1500.

4-8. STATUS OF EMPLOYEE AFTER OWCP CLAIM IS FILED

Claims for compensation are typically time consuming and, once submitted, can take anywhere from a few months to more than a year before a decision is rendered by OWCP. This situation obviously presents problems to both the employee and the supervisor. To appreciate the implications of the delay in receiving a decision, the following information is offered:

a. Claim is Pending. Under this status, the employee will presumably have used and, in all likelihood, exhausted, the 45-day COP related to a traumatic, job-related injury. The employee has the option of using a combination of sick and annual leave after the 45-day period. He/she may also request and be approved for leave without pay (LWOP) pending a determination by OWCP. If OWCP approves the claim, a "buy back" provision exists for the leave utilized while the claim was pending.

b. Claim is Disapproved by OWCP. Under this situation, whatever leave was utilized by the employee is lost without reimbursement. Further, OWCP may rule the use of 45 days of COP was wrongfully requested/utilized and retroactively deny COP and require repayment.

c. Claim is Approved by OWCP. Under this situation, the employee's status will require submitting various documents requested by OWCP, keeping the supervisor informed of his/her status, and receiving compensation until return to duty.

(1) If the employee's disability is total but temporary, the supervisor must plan for the employee's ultimate return to duty. Within NCIS, this creates obvious manpower problems. By law, the employee is guaranteed a return to his/her position, or, its equivalent, at any time within one (1) year from the start of compensation. An equivalent position is defined as one for which the employee is fully qualified and which has the same seniority, status and pay as the prior position.

(2) A permanent total disability entitles the injured employee to compensation until death. Rates of compensation are included in the linked documents.

d. Fitness for Duty. Before the employee can be allowed to return to work, he/she may have to undergo a fitness-for-duty examination. If, for whatever reason, the employee fails to successfully complete that examination, an application for disability retirement should be filed with the Office of Personnel Management via Code 10A and S/HHRO.

4-9. DEATH IN THE LINE OF DUTY

Information on the procedures to be followed and the accrued benefits, in the event an employee dies in the line of duty, may be found in Title 20 Code of Federal Regulations Part 10.

4-10. BURIAL BENEFITS

Burial Benefits, not to exceed $800, may be paid for funeral and burial expenses of the employee whose death resulted from injuries received on the job. If the employee dies away from his/her area of residence, the cost of transporting the body to the place of burial will be paid in full. Itemized funeral bills should be submitted to OWCP for consideration of payment or reimbursement. Additionally, when death occurs while an employee is traveling on official business or during a TDY assignment outside CONUS, or while at the official station outside the United States, actual costs for preparation of the remains of the employee will be allowed (this provision is covered by the Joint Travel Regulation (JTR, Vol II.). In addition, a $200.00 allowance will be paid in consideration of the cost of terminating the deceased status as a Federal employee.

CHAPTER 5
TITLE: INSPECTOR GENERAL MATTERS
POC: CODE 00I
DATE: SEP 07

POLICY DOCUMENT
APPENDIX (1): Gen Admin 11C-0011 of 28 May 2013 released NCIS Policy Document 13-04: Administrative (External Inspector General (IG) and Audit Services Requests for Information and Assistance). Policy Document 13-04 contains revised or new policy that has not been incorporated into this chapter and should be reviewed in its entirety.

5-1. GENERAL

The NCIS Office of the Inspector General (OIG), NCIS Code 00I, headed by an Inspector General (IG), is responsible for providing oversight to the efficiency, effectiveness, and integrity of NCIS operations and personnel. This responsibility is performed through implementation of a multi-faceted inspection process, Managers' Internal Controls Program, Intelligence Oversight Program and by conducting internal inquiries and investigations of allegations of misconduct by NCIS personnel. The NCIS IG shall be a GS-15 or higher, appointed with the concurrence of the Naval Inspector General, reporting directly to the Director, NCIS, and be assigned additional duty to the staff of the Naval IG in accordance with SECNAVINST 5430.57 (series). This chapter establishes NCIS policy and procedures for these programs.

5-2. COMPLAINT REPORTING

The NCIS IG investigates allegations of waste, fraud, abuse, mismanagement, and misconduct by NCIS personnel. All inquiries into matters affecting the readiness, integrity, discipline and efficiency of NCIS shall be conducted in an independent and professional manner, without command influence, pressure or fear of reprisal from any level within the DON. Complaints should be forwarded via letter, e-mail, facsimile, or telephone to the IG, Deputy IG, or Investigations Division Chief.

5-3. INTERNAL PERSONNEL INVESTIGATIONS (IPI) (CATEGORY 2B)

5-3.1. Requirement. It is occasionally necessary to make official inquiries into allegations of personnel misconduct. Such inquiries are mandatory when the actions of special agents or other personnel, involve breaches of NCIS policy or doctrine, violations of criminal law, or are of such nature to bring serious discredit on NCIS or the United States Navy. Prompt, thorough, and

objective investigations of such allegations or situations are of extreme importance because of the impact on the reputation of the individuals involved and the professional reputation and effectiveness of NCIS. This is of particular significance with the special agent corps because the criminal investigator is uncommonly vulnerable to specious, self-serving accusations of wrongdoing by criminal suspects or subjects of investigations. This is a recognized diversionary or recriminatory tactic. It is mandatory to ensure that the official conduct of all NCIS personnel be in total conformity with appropriate law, regulation and policy. For these reasons, it is necessary that NCIS establish a standard procedure for the conduct of IPIs to ensure that fair, impartial, and thorough inquiries are conducted, and to provide an accurate and objective record on which supervisory judgments can be based.

5-3.2. Policy. The policy set forth below will apply when it is reported, alleged or reasonably suspected that special agents or other NCIS personnel are involved in serious acts of misconduct, violations of law or breaches of NCIS policy or doctrine which, if true, could possibly result in formal disciplinary action against those involved. This is to include incidents wherein it is known that a policy or doctrine was breached but the identities of NCIS personnel or the extent of their involvement has not been established.

a. The NCIS OIG shall be the initiating authority for all IPIs. Upon receipt of substantive information alleging or otherwise indicating involvement by special agents or other NCIS personnel in misconduct as described above, the known facts will be provided to the OIG by the fastest means available. The NCIS IG will determine whether a formal IPI is warranted. The NCIS IG will report allegations of whistleblower reprisal or wrongdoing by senior NCIS officials to the DoD/Naval IG as required by DoD/DON instructions. The NCIS IG will advise the Naval IG prior to initiating any inquiry deemed reasonably likely to be of interest to the Secretary of the Navy (SECNAV), the Chief of Naval Operations (CNO), the Commandant of the Marine Corps (CMC) or Congress. The NCIS OIG has the authority to use all resources of the agency to complete investigations and will control all IPIs. The OIG will identify the special agent(s) who will control the IPI and provide guidance as to the scope of the investigation. The OIG will also assign a NCIS Headquarters (NCISHQ) case control number and establish the priority of the investigation. The primary case agent will be responsible for producing the ROI (OPEN) and ROI (INTERIMs).

b. IPIs will be reported by ROI under NCIS case category 2B. All documentation for category 2B investigations will be forwarded directly to Code 00I in an inner sealed envelope with external instructions that the envelope is to be opened only by the NCIS IG. The standard NCIS reporting format (i.e. SSD) will be used for all IPI reporting, however, transmission via the SSD system is not to be utilized. The only authorized means of transmission of IPI reporting is mail, express delivery, facsimile or e-mail. In those cases where facsimile transmissions of IPI documentation are required, all involved components will be alerted separately to ensure that disclosure of the contents of said documentation is limited to those with a strict need-to-know. Generic titles are acceptable; however, when an investigation obviously is centered on the misconduct of a certain NCIS member(s), the title block shall contain the name(s) of the member(s). At the conclusion of the investigation, all case notes from any agent/office involved in the investigation shall be forwarded to the NCIS OIG for retention.

c. NCIS personnel who are believed to be witnesses in a matter under investigation are required to cooperate in the investigation. This cooperation includes the execution of signed, sworn statements if such are deemed appropriate by the investigating personnel. NCIS personnel who are under investigation concerning matters relating to their professional duties are likewise required to account for their acts or failure to act in connection with their duties. A failure to cooperate is considered a serious matter adversely impacting on the employer/employee relationship. In the case of civilian personnel, such a failure to cooperate could lead to formal disciplinary action, including removal from federal service.

d. The NCIS IG will, to the maximum extent permitted under law and regulation, safeguard the identity of complainants. NCIS IG investigators shall explain to complainants that the use of their testimony and the release of their identities as witnesses, but not as complainants, may be necessary under due process procedures associated with disciplinary or administrative action.

e. The NCIS IG will, to the maximum extent permitted under law and regulation, safeguard the identity of witnesses and assist them, as appropriate, if it is determined by the NCIS IG that they are victims of reprisal. NCIS IG investigators shall explain to witnesses that it may be necessary under due process procedures associated with disciplinary or administrative action to release their identity. Such identifications will be made only to those with an official need to know the identity of the witness.

5-3.3. Purpose. The purpose of the IPI is to:

a. Clarify all serious issues regarding NCIS personnel misconduct. This includes both acts of commission or omission.

b. Establish the merit or lack of merit of all allegations, accusations or suspicions of NCIS personnel misconduct.

c. Collect all available information and reports compiled by other agencies, when such agencies are investigating NCIS personnel for violations of criminal law.

d. Document all incidents where a duty weapon, or personal weapon authorized for use as a duty weapon, is discharged, accidentally or intentionally, other than during the firearms qualification process or in combat zones when the rules of engagement have been followed.

e. Identify all culpable parties.

f. Collect all pertinent supportive evidence: real, physical and circumstantial.

g. Resolve clearly and completely all reasonable accusations, allegations and suspicions directed against NCIS personnel regardless of the nature of the incident or issue and regardless of culpability.

h. Fully document NCIS practices and/or procedures approved or otherwise, which may have contributed to the incident or issue.

5-3.4. Jurisdiction in Criminal Matters. In those IPIs involving alleged violations of criminal law by NCIS personnel, the prevailing investigative jurisdictional requirements or agreements will pertain. When the agency of primary jurisdiction defers that jurisdiction to NCIS, the matter will be pursued in accordance with existing NCIS criminal investigative policy by the cognizant field office and monitored by the OIG. Before opening a criminal investigation involving an NCIS employee, the field office should coordinate with the NCIS OIG. The NCIS IG will decide whether to assume responsibility for the criminal investigation and/or conduct a parallel IPI in addition to the criminal investigation based on suspected violations of agency policy, procedure or regulations. In all cases, the matter will be discussed as soon as practicable with the appropriate judicial office in order to determine prosecutive interest. Normally, the ROIs will be provided to such judicial office unless that office or other properly constituted authority has specifically declined prosecutive interest. IPIs that monitor and report progress of criminal investigations conducted by other agencies will contain, as attachments, copies, or summaries (in Investigative Action format) of all of the other agencies' reports.

5-3.5. Counterintelligence Scope Polygraphs. When a NCIS employee undergoes a counterintelligence scope polygraph (CSP) and registers either significant physiological response (SR) or no opinion (NO), and all avenues to resolve the issues available to the polygraph examiner have been exhausted, an immediate referral to the NCIS OIG will be made and an IPI is initiated. The OIG will also notify NCIS Code 22 of NCIS employees who fail their CSP. Should the IPI surface indications of specific national security violations associated with espionage or other national security concern, the NCIS IG, in conjunction with NCIS Code 22, may task the Office of Special Projects (OSP) or other field office component to conduct a counterintelligence investigation into the matter.

5-3.6. Administrative Use of the IPI.

The ROI (Interim) in IPIs will be forwarded by the NCIS IG to the Deputy Assistant Director (DAD) (Personnel Operations and Services) and the appropriate Special Agent-in-Charge (SAC)/NCISHQ DAD. The SAC/DAD will forward a recommendation for disposition of the matter via letter to the DAD (Personnel Operations and Services). The DAD (Personnel Operations and Services, NCIS Code 24B) will process the matter in accordance with NCIS-1, Chapter 18. The NCIS IG will also review the completed IPI investigation, when NCIS procedures and practices are at issue, for purposes of recommending changes to those procedures and practices.

5-3.7 Search of Command Computer And Communications Systems And Related Media.

In support of the IPI investigative process, the NCIS IG may authorize the search and/or seizure of command owned, operated or leased classified and unclassified computer systems and related electronic media, data storage systems and communications systems. This includes, but is not limited to, government issued, leased or rented mobile phones, satellite telephones, personal data assistants (PDA’s), desktop and laptop computer systems and servers.

5.3.8 Placing Special Agent Personnel in Limited Duty Status

The NCIS IG, or other authorized official, may place a special agent on a limited duty status if the individual is the subject of an IPI and the allegations raise questions of the special agent's judgment, integrity or competence. Additional guidance is found in NCIS-1, Chapters 13-19.

5.3.9. NCIS IG Database Inquiries.

Databases maintained by the OIG may, upon request from competent authority, be reviewed for any information on employees (past and present) who are being considered for reassignment, transfer, training, awards or security clearance eligibility.

5.3.10. Personnel Security Review Board (PSRB).

The PSRB exists to assist and advise the NCIS Security Manager on a variety of personnel security related issues. The NCIS IG, or designee, will be a member of the PSRB.

5-4. NCIS IG INQUIRIES (CATEGORY 2C)

The NCIS IG is authorized to conduct inquiries (investigations, inspections, examinations, studies or audits) in support of, or at the request of, the Director, NCIS, or as part of a fact-finding process in response to a DoD/DON hotline or other referral. These inquiries will be documented using case category 2C.

5-5. INSPECTIONS

The requirement for an inspection program is inherent to the function of a professional law enforcement and counterintelligence agency. The exercise of authority includes establishment of such inspection processes as may be necessary to verify that tasks or missions are being properly accomplished. SECNAVINST 5400.14 (series) provides authority and responsibility for administration of DON shore activities, including the responsibilities of planning and inspection. SECNAVINST 5040.3 (series) promulgates the DON Inspection Program which levies inspection requirements on DON organizations. Essentially, inspections of subordinate components of DON commands shall be periodically conducted.

5-5.1. Policy.

a. The Director, NCIS desires an effective and meaningful inspection program. The NCIS inspection program will primarily focus on the core functions of investigations, operations and related support activities.

b. The NCIS inspection program is the specific responsibility of the NCIS IG.

5-5.2. Objectives.

The objectives of NCIS inspections are to:

a. Assess leadership.

b. Assess quality of investigative and operational activity.

c. Assess effectiveness and efficiency of NCIS components.

d. Assess staffing levels.

e. Assess quality and management of available resources.

f. Assess compliance with established policies and procedures.

g. Evaluate anomalies which prevent or inhibit compliance to established policies and procedures.

h. Develop appropriate recommendations to correct deficiencies.

5-5.3. Definitions.

a. NCISHQ Inspections. Formal inspections of NCISHQ and field components by representatives of NCISHQ under the direction of the NCIS IG.

b. Field Office/Departmental/Geographic Executive Assistant Director Inspections. Inspections conducted by NCIS field office, NCISHQ departmental management personnel or geographic EADs of subordinate components. Included are self-inspections by subordinate Resident Agents-in-Charge (RAC) and Supervisory Special Agents (SSA) and validation of those self-inspections by field office managers.

c. Field Office Management Visits. Official in-person visit by a SAC, ASAC or RAC of the NCIS field office management team at a subordinate component. These management visits must be made to each subordinate component on a semi-annual basis. Results of Field Office Management Visits will be formally documented via letter from the SAC to the NCIS IG. Inspection/ visit report protocols are posted on the NCIS IG's website http://infoweb.ncis.navy.mil/agency/deptwebsites/ig/ig-index.html.

5-5.4. Duties of Inspectors. The NCIS OIG maintains a cadre of personnel available to conduct triennial and follow-up inspection visits to field offices and headquarters departments. The NCIS IG may augment the inspection team using personnel from various field offices or headquarters departments as necessary. Typically, augmentees to the NCIS IG inspection team will be at the SSA level or above.

a. Basic duties of Inspectors is to:

(1) Determine if the component is fulfilling the NCIS mission.

(2) Assess if fundamentally sound investigations and operations are being conducted.

(3) Evaluate indigenous conditions that indicate alternatives or waivers to established policies and procedures may be warranted to enhance efficiency of inspected component.

(4) Evaluate and report facts accurately, concisely, and intelligently.

(5) Provide whatever background information is necessary to assist reviewers in an analysis of the facts.

(6) Draw proper conclusions from facts obtained.

(7) Make logical, unbiased recommendations for appropriate corrective action.

(8) Coordinate all inspection findings with the NCIS IG.

b. In order to carry out these duties effectively, inspectors should prepare themselves in advance by:

(1) Taking part in pre-inspection briefings and planning evolutions.

(2) Studying the geographic jurisdiction, resources and assigned tasks of the component to be inspected.

(3) Consulting previous inspection reports of the component involved.

(4) Reviewing inspection guides and identifying any additional appropriate topics that should be covered.

(5) Conducting a thorough analysis of the workload of the component to be inspected.

5-5.5. NCISHQ Inspection Procedures.

a. Scheduling.

(1) A headquarters inspection of each field office and headquarters department will be scheduled triennially, with follow-up inspections conducted as deemed appropriate. These inspections shall include as many subordinate offices as feasible. Where necessary, limited inspections of some offices may be conducted when factors prevent complete coverage. Inspection schedules are published on the NCIS IG's website on the NCIS INFOWEB.

(2) The NCIS IG may conduct an unannounced or short notice inspection of any NCIS component at any time.

b. Arrangements.

(1) The NCIS IG will normally advise the field office SAC of the scheduled inspection dates 45 - 60 days in advance to allow for proper planning. Alternate dates may be proposed, if warranted.

(2) If requested, all necessary administrative arrangements (e.g., local transportation, billeting, etc.) shall be made in advance by the component to be inspected.

(3) The inspected component will arrange protocol and liaison visits considered appropriate by the inspector(s). SACs are encouraged to arrange visits that may enhance relationships or otherwise be beneficial to the inspected component.

c. Headquarters Inspection Team Composition.

(1) The NCIS IG will direct inspectors' activities and report inspection results to the Director, NCIS.

(2) Inspection teams shall be comprised of personnel designated by the NCIS IG. The size and location of component(s) to be inspected and complexity of workload will be taken into account by the NCIS IG in determining the size of the inspection team.

(3) As stated above, the NCIS IG may task field office SACs and NCISHQ DADs to provide personnel to participate in NCIS IG inspections as warranted.

d. Initial Briefing. The field office SAC or designee shall be prepared to present a pre-inspection briefing to the inspection team. The briefing should acquaint the team with the overall organization, workload, and performance plan of the inspected component, and any problem areas pertinent to the inspection. For inspections of subordinate components, the senior manager should provide the briefing. Briefings may be omitted if deemed unnecessary by the NCIS IG or the senior inspector present.

e. The Inspection.

(1) General areas/items to be inspected: In support of the objectives cited above, members of the inspection team will concentrate on:

(a) The component's performance, productivity, planning and programming with respect to investigations and operations.

(b) The type and level of support the component provides and is provided by commands in its area.

(c) Whether the component's personnel allowances should be augmented, reduced or consolidated to ensure the most efficient and effective use of manpower (staffing assessment).

(d) Pertinent aspects of leadership, morale, management, use of resources and training at the component.

(e) Component compliance with prior inspection recommendations.

(2) Specific items/areas. Inspectors will <u>specifically</u> address investigative and operational oversight, leadership, morale, staffing and production assessments, training, investigative support, resource management, and office administration. Additionally, inspectors will validate

selected items or sections of the inspected component's previously completed self-inspection report.

(a) The inspectors' inquiries should include broad-ranging discussions with personnel knowledgeable of the component, covering such topics as:

1. Current problems requiring assistance from higher authority.

2. Situations or practices which actually or potentially detract from performance.

3. Whether there are functions or tasks levied on the component without concomitant resources.

4. Plans or projects which have or will result in economies or increased effectiveness.

(b) Inspectors do not have supervisory authority over inspected components and must guard against actions that could be interpreted as attempts to exercise such authority. Suggestions for improved efficiency can and should be made by the inspectors.

(3) Use of Inspection Guides

(a) The inspection guides, posted on the NCIS IG website, have been developed as tools for inspectors (and field office managers). They should be considered as suggestive of major areas of inquiry, not as inflexible checklists.

(b) There is no prohibition against including additional items that local conditions suggest would be meaningful. The good judgment and common sense of inspectors will dictate those items that require in-depth examination in order to meet the objectives of the inspection.

(4) Inspection Evaluations

(a) The most significant measures of a component's performance are the quality of its leadership, sustained mission accomplishment and adherence to established policy. It is essential inspectors base their inspections and recommended evaluations on the premise of an ability to accomplish the mission, use of resources, and adherence to existing policy and procedures. Extraordinary circumstances or conditions outside the control of the inspected component interfering with mission accomplishment should be addressed.

(b) In keeping with DON policy, only "Satisfactory" or "Unsatisfactory" evaluations will be assigned as overall grades in headquarters inspections of NCIS components. A "Satisfactory" evaluation shall be assigned whenever mission accomplishment meets or exceeds minimum standards. An "Unsatisfactory" evaluation shall be assigned when mission accomplishment is below minimum standards; the component is evaluated incapable of performing its assigned functions, or is in blatant violation of basic NCIS policy. The assignment of an "Unsatisfactory" evaluation to any functional area or to any inspected component must be fully supported in the inspection report, and must be accompanied by recommendations necessary to improve

performance to an acceptable level. "Unsatisfactory" evaluations are subject to follow-up inspection by the OIG.

(5) Special Interest Items. The Naval Inspector General periodically publishes OPNAVNOTEs which designate "Items of Special Interest" to the SECNAV and CNO. These items must be inspected as part of NCIS headquarters and field office inspections. All of the special interest items might not pertain to the type or specific component being inspected.

(6) Critiques. A post inspection critique is an essential part of NCIS inspections. The critique offers inspectors an opportunity to personally discuss their findings with senior personnel of the inspected component. The depth and scope of the critique will depend on the type of inspection involved and on the inspector's level of authority. For headquarters inspections, the critique of the field office will be in detail and may include direction for corrective action. Critiques should address all matters of mission accomplishment arising from the inspection, and all major issues relating to conformity with applicable regulations or standard operating procedures. Inspectors conducting headquarters inspections of the field office's subordinate components shall also provide a detailed critique to the senior manager.

f. Headquarters Inspection Reporting and Follow-Up.

(1) Reports of Inspections

(a) One report of inspection will be promulgated for the field office/headquarters department. The report will summarize those topical areas previously identified in section 5-5.5.e. and how they impact on the conduct of fundamentally sound investigations and operations. The report will also contain general observations by inspectors of individual components; a staffing and production assessment; Navy Special Interest Items; and formal findings and recommendations.

(b) Findings and recommendations relating to significant matters will be listed in the inspection report and each will be assigned a unique identifying number to assist in tracking follow-up actions.

(c) Once approved by the NCIS IG, the completed inspection report will be forwarded to the SAC/DAD within 45 days. Every effort shall be made to keep the inspection report at the unclassified level.

(2) Follow-Up

(a) Proper follow-up to ensure that appropriate action is taken on recommendations resulting from inspections is a natural adjunct to an inspection program.

(b) The SAC/DAD of a component undergoing a headquarters inspection shall, within 45 days of receipt of the inspection report, submit to the NCIS IG a report on actions taken, in progress, or proposed to correct all deficiencies and satisfy all recommendations listed in the report. If the corrective action is pending, a final response is required when the action is completed.

(c) A re-inspection shall be conducted whenever a grade of "Unsatisfactory" is assigned, or when a significant number of major discrepancies are reported. A major discrepancy is defined as a condition or omission that has an adverse impact on mission accomplishment or the operation of any major functional area, and includes significant non-compliance with policy directives and/or deviation from accepted standards of prudence. Timing of re-inspections is at the discretion of the NCIS IG.

(d) Where NCISHQ elements are action components for inspection recommendations, the NCIS IG will notify the headquarters element by memorandum, which will include a suspense date.

5-5.6. Field Office/Departmental Inspections.

a. Responsibility. SACs and DADs are primarily responsible for mission accomplishment and monitoring the quality and timeliness of NCIS investigations and operations. SACs/ DADs are empowered to ensure subordinate managers are also held accountable for that responsibility at subordinate components. A critical tool at the SAC's/DAD's disposal is the self-inspection report. During management visits it is imperative that particular attention be paid to mission accomplishment and the review of the investigative/operational product for quality and timeliness.

b. Self-Inspections

(1) Each field office component and headquarters department is required to conduct a self-inspection each year and report the results to the OIG. The Self-Inspection Program is the component of the NCIS Inspection Program that provides the Director, NCIS with the annual assurances that field operations are in compliance with DoD, DON, and NCIS policies, directives and regulations. These self-inspections serve as input to the Director's NCIS annual Statement of Assurance to the SECNAV that NCIS has a system of internal controls in place and the objectives of the Federal Managers' Financial Integrity Act are being achieved.

(2) The SSA at the NCISRA or co-located operational field office elements will certify to the SAC by signature and date of the self-inspection report that the inspection items identified in the NCISRA inspection guide (posted on the NCIS IG website) have been addressed. Using the Self-Inspection Questionnaire (SIQ), SACs/DADs conduct a comprehensive review of their programs, to include subordinate offices, by addressing the questions contained in the ten sections or core areas. All sections of the self-inspection guide should be addressed or noted as "not applicable" if appropriate. SACs/DADs must then assess and evaluate their compliance with the core areas by completing the self-rating and certification forms. The sections certified or evaluated as either "Acceptable - Needs Improvement" or "Unacceptable", require the SACs/DADs to develop a corrective action plan by completing the Corrective Action Certification form. In doing so, actions to be corrected, completion dates and supervisors/managers to monitor their progress are required. Once the non-compliance issues are corrected, the SACs/DADs will certify their completion.

(3) The self-inspection forms for both the field office and NCISHQ department are located on the NCISnet OIG website. SACs must complete the field office SIQ, Self-Rating Certification and Corrective Action Certification, if applicable. The DADs are required to complete the headquarters SIQ, Self-Rating Certification and Corrective Action Certification, if applicable. All SIQ forms can be downloaded from the NCISnet, homepage address http://infoweb.ncis.navy.mil/agency/deptwebsites/ig/ig-forms.html.

(4) The field office and NCISRA/NCISRU self-inspection reports shall be maintained at the field office for two years. A copy of all field office and NCISHQ department self-inspection reports are to be forwarded annually to the OIG along with the SAC's/DAD's comments and Corrective Action Certification Forms by 31 March of each year.

5-5.7. Semi-Annual Management Visits.

a. The SAC, operational ASACs or RACs of the field office management team must conduct a management visit to each subordinate component semiannually. During these management visits, the visiting manager(s) will validate the component's self-inspection report. It is the SAC's discretion to validate the entire self-inspection report during one visit or cumulatively over the semiannual visits. Flexibility is suggested in the intensity/detail of coverage within each of the inspection guide's captioned areas to better meet management needs.

b. Field Office management visit reports must be submitted to the OIG within 30 days of the visit in order to meet Naval IG quarterly reporting requirements imposed on NCISHQ. This report should be a short narrative style memorandum identifying components visited and any significant issues identified.

c. The SAC may designate other field office managers to assist in semi-annual visits as appropriate; e.g., ASACs should conduct visits of their subordinate NCISRAs. However, at least once yearly, each field office component must be personally visited by the SAC. Extraordinary circumstances (exigent operational requirements; funding constraints, etc.), which may preclude semi-annual management visits, must be coordinated with the NCIS IG.

d. Although private interviews will not be a requirement of each visit, assigned personnel should be afforded the opportunity for such interviews to the extent practicable or if specifically requested.

e. In conjunction with the semi-annual visits, field office management will address intelligence oversight requirements (i.e., Executive Order 12333) with each component at least once a year. These discussions will be documented as appropriate in the visit report to the OIG.

5-5.8. Inspections by NCISHQ Departments.

For NCISHQ departments exercising operational control of field components, e.g., NCIS Code 22 for the Office of Special Projects and NCIS Code 24 for Contingency Response Field Office, Cyber, polygraph and technical support elements, the inspection and reporting requirements are

the same as for field offices.

5-5.9. Inspections of NCISHQ Departments.

a. All NCISHQ departments will be inspected on a periodic basis. Like the inspections conducted of the NCIS field components, the inspections conducted of NCISHQ departments will focus on core functions. Of primary importance is the quality of the service that the NCISHQ departments are providing to their various customers and particularly to the field components in support of investigations and operations.

b. The objectives of NCISHQ departmental inspections and the duties of the inspectors are fundamentally the same as those associated with the inspections of field components as enumerated in sections 5-5.2 and 5-5.4 above.

c. Scheduling. Each of the NCISHQ departments, like NCIS field components, will be scheduled for inspection triennially. The NCIS IG will be responsible for the scheduling of those inspections. The inspection schedule is posted on the NCIS IG's website available on the NCISnet, http://infoweb.ncis.navy.mil/agency/deptwebsites/ig/ig-index.html

d. Arrangements. The NCIS IG will normally coordinate with the Assistant Director of the department to be inspected 45-60 days in advance to allow for personnel availability and other planning requirements.

e. Inspection Team Composition. Inspection teams conducting NCISHQ departmental inspections shall be comprised of personnel designated by the NCIS IG. As in the case of the inspection of NCIS field components, the NCIS IG may use personnel assigned to other NCISHQ departments and/or may task field office SACs to participate in or provide subordinate personnel to take part in the inspection of NCIS headquarters departments.

f. Initial Briefing. The AD of the NCISHQ department to be inspected or designee shall be prepared to present a pre-inspection briefing to the inspection team. The briefing should acquaint the team with current data relative to program objectives, organizational structure and functions, staffing, support to the field, future plans and any problem areas pertinent to overall program management. As coordinated in advance between the NCIS IG and the AD of the department to be inspected, the pre-inspection briefing may be given to the entire inspection team or to designated inspection team members only. Briefings may be omitted if deemed unnecessary by the NCIS IG.

g. The Inspection.

(1) General areas/items to be inspected. In support of the objectives cited above, members of the inspection team will concentrate on:

(a) The department's performance, productivity, planning and programming with respect to its mission responsibilities.

(b) The quality and timeliness of the support that it provides to the NCIS field components.

(c) Whether the department's personnel allowances should be augmented, reduced or consolidated to ensure the most efficient and effective use of personnel (staffing assessment)

(d) Pertinent aspects of leadership, morale, management, use of resources and training within the department.

(e) Departmental compliance with NCIS policy, other relevant instructions and prior inspection recommendations.

(2) Specific Items/Areas. Inspectors will specifically address; management oversight of program responsibilities, the quality and timeliness of support provided, resource management, morale, training, staffing and production assessments, department administration, plans and policy, and Navy special interest items. Other areas may be included in the above list as deemed appropriate by the NCIS IG.

(a) Inspectors will validate selected items or sections of the inspected department's previously completed self-inspection report.

(b) Inspectors assigned to take part in the inspection of NCISHQ departments will attempt to interview the broadest possible range of employees. If the number of departmental personnel is such that it is not feasible to interview each employee, the inspectors will identify for interview those assigned to key areas and those that are believed to have pertinent information. In addition, any employee of the department who specifically requests to speak with the inspectors will be interviewed.

(c) Interviews with department employees will cover a wide spectrum of topics relative to the general areas/items of interest identified above. Of particular interest to the inspection team will be employee input that would assist in the identification of:

1. Unique solutions to problems within the inspected department which may also be common to other NCISHQ departments.

2. Problem areas or perceptions of problem areas not previously communicated to department managers.

3. Situations or practices which actually or potentially detract from individual or departmental performance.

4. Resource shortfalls which may be negatively impacting on mission accomplishment.

5. Problem areas or program planning efforts that might benefit from an interdepartmental approach.

(d) As in the case of the inspection of field components, the inspection team members do not have supervisory authority over personnel in the inspected department and, as such, should avoid actions that could be interpreted otherwise. Significant inspection findings, whether positive or negative, will be communicated to the NCIS IG or his/her designee and not directly from inspectors to personnel of the inspected NCISHQ department. The NCIS IG is solely responsible for the development, coordination and communication of inspection findings and recommendations.

h. Use of Inspection Guides. The attached NCISHQ Departmental Inspection Guide provides information to expand upon the general areas and specific items of inspection interest listed above.

i. Inspection Evaluations.

(1) The most significant measures of a department's performance are generally the same as those used to evaluate the operational field components. The quality of the leadership of the department is of major importance, as are the department's ability to demonstrate sustained mission accomplishment and its adherence to established policy. In determining the level of performance in these critical areas, inspectors will evaluate the level of support provided to the department's internal and external clients, the clarity of its program guidance, and other relevant criteria.

(2) As in the inspection of NCIS field components, only "Satisfactory" and "Unsatisfactory" evaluations will be assigned. All related definitions and requirements for the evaluation of NCIS field components apply equally to the evaluation of NCIS headquarters departments.

5-6. MANAGERS' INTERNAL CONTROLS (MIC) PROGRAM

Managers are responsible for ensuring that resources under their purview are used efficiently and effectively, and that programs and operations are discharged with integrity and in compliance with applicable laws and regulations. The MIC Program is one tool available to assist them in this duty. The NCIS IG is the designated NCIS Program Manager. SACs/DADs are designated as Assessable Unit Managers with responsibility and accountability for establishing and assessing internal controls in their subordinate elements in accordance with the NCIS Managers' Internal Controls Program Plan. The internal controls program plan can be located on the NCISnet http://infoweb.ncis.navy.mil/agency/deptwebsites/ig/documents/mgmtctrlplan.pdf.

5-7. INTELLIGENCE OVERSIGHT

a. Intelligence oversight is broader in scope than simply the protection of U.S. persons' rights and privacy from intrusion by intelligence activities and agencies. Intelligence oversight includes assurance that all NCIS intelligence activities, operations, and programs function in compliance with applicable U.S. law, statute, directive, and policy.

b. The NCIS IG is responsible for administering the Intelligence Oversight Program within NCIS and is the primary point of contact for all intelligence oversight matters, to include submission of quarterly reports, inspections and investigations, and clarification of regulations.

c. Within each NCIS field office; the ASAC with responsibility for the Counterintelligence Program is designated as the Field Office Intelligence Oversight Officer. Within each NCISRA, the SSA is designated as the Unit Intelligence Oversight Officer. Intelligence Oversight Officers are responsible for ensuring required training is completed, answering employees' questions regarding authorized activities, and forwarding reports of questionable activity to the NCIS IG.

5-7.1. Responsibilities/Reporting Of Questionable Intelligence Activity.

a. Under DoD Regulation 5240.1-R, NCIS employees are assigned the responsibility to conduct only lawful intelligence activities.

b. A questionable intelligence activity is one that may violate the law, any Executive Order (such as E.O. 12333, United States Intelligence Activities), Presidential directive or applicable DoD policy (such as DoD 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons). Examples of a questionable intelligence activity include, but are not limited to, the following:

(1) Alleged abuse and mistreatment of detainees and prisoners by or directed by intelligence personnel.

(2) Tasking intelligence personnel to conduct intelligence activities that are not part of the organization's approved mission, even if they have the technical capability to do so.

(3) Providing intelligence services and/or products without proper authorization.

(4) Failure to file proper use statements for imagery collection associated with U.S. persons.

(5) Collecting information on U.S. persons, even though open source, when it is not part of the unit's mission.

c. NCIS employees must report questionable intelligence activities to one of the following:

(1) Immediate Supervisor.

(2) NCIS Legal Department.

(3) NCIS OIG.

5-7.2. Reporting Requirements to Naval IG.

a. Quarterly Requirements. NCIS is responsible for providing a quarterly intelligence

oversight report regarding any questionable activities conducted by or on behalf of NCIS to the Naval Inspector General's office (NAVINSGEN N2) no later than the 15th of the month following the end of the quarter.

b. Annual Requirements. NCIS is responsible for providing an annual intelligence oversight report to the Naval Inspector General's office (NAVINSGEN N2) no later than the 15th of the month following the end of the calendar year. The report will include the intelligence oversight inspection schedule for the following fiscal year.

5-7.3. Training Requirements. SECNAVINST 3820.3E requires Navy intelligence components to train new employees on intelligence oversight and to conduct and document refresher training at least annually. Intelligence oversight training is required for all special agents, intelligence specialists, office managers, field investigative assistants, field office support officers and all employees of the Intelligence Directorate, Combating Terrorism Directorate, Counterintelligence Directorate, Cyber Department and Legal Department. The in-service training for NCIS can be found on the Code 10B or NCIS IG website. The Field Training Coordinator or the NCISHQ Training Coordinator will report the results of the intelligence oversight training to Code 10B.

5-7.4. Inspections. The Assistant to the Secretary of Defense for Intelligence Oversight (ATSD-IO) and the Naval Inspector General conduct regular inspections/visits to ensure that the inspected activity is in compliance with oversight regulations. In addition, the NCIS IG will assess compliance with intelligence oversight policy during inspections of NCIS elements.

APPENDIX (1)

660331 12:58 20130528 IN:SSDEMAIL #105213 OUT:NCISWWSSD #1098

GENERAL ADMINISTRATION 28MAY13

FROM: 0000 GEN: 11C-0011

TO: DIST

SUBJ: NCIS POLICY DOCUMENT 13-04: ADMINISTRATIVE (EXTERNAL INSPECTOR GENERAL (IG) AND AUDIT SERVICES REQUESTS FOR INFORMATION AND ASSISTANCE)

1. This policy document establishes new procedures when Naval Criminal Investigative Service (NCIS) personnel receive a direct request for information or assistance from representatives of Federal, Department of Defense (DoD), and Department of the Navy (DON) Inspector General and Audit Services (e.g., FBI Office of Professional Responsibility, DoD Inspector General (DoDIG), Naval Inspector General (NAVINSGEN), Naval Audit Service (NAVAUDSVC), etc.). In the past, NCIS has received requests from these agencies at several levels of the NCIS chain of command and, in some cases, direct requests to the field. Frequently these requests are misdirected, misplaced, and can be wastefully redundant. This is inefficient and can impede the processing of the information or assistance requested. The new procedures will enable NCIS to provide an efficient and timely response for these requests.

2. To coordinate and accommodate these requests, the following is effective immediately:

a. All requests for information or assistance coming from the DoDIG, NAVINSGEN, NAVAUDSVC, and other Federal IG/Audit Services, except in those areas where NCIS is working joint investigations (i.e., fraud-related investigations), will be coordinated by the Assistant Director (AD) for Inspections (NCIS IG) or his/her designee.

b. An NCIS employee who receives a request for information or assistance from an external IG or Audit Service, except in joint investigative matters (i.e., fraud-related investigation), will immediately notify his/her supervisor of the request, who will relay the information to the AD for Inspections.

c. The AD for Inspections will coordinate the needed information or assistance requested with the appropriate NCISHQ or field office. This coordination may be accomplished via telephonic or e-mail communication.

3. Nothing in this guidance is intended to discourage or prohibit employees from their legal right to initiate hotline complaints with any IG's office. The intent of this policy is to improve coordination of external IG and Audit Service requests coming in to NCIS.

4. This policy will be incorporated in the next revision of NCIS-1,

28MAY13

SUBJ: NCIS POLICY DOCUMENT 13-04: ADMINISTRATIVE (EXTERNAL INSPECTOR

Chapter 5, Inspector General Matters.

5. Questions regarding this policy may be directed to (b)(6), (b)(7)(C) Acting Inspector General, who may be reached at (b)(6), (b)(7)(C) @navy.mil or (b)(6), (b)(7)(C) (b)(6), (b)(7)(C)

DISTRIBUTION
NCISHQ: ALL DIRECTORATES AND DEPARTMENTS
INFO: WWSSD

NCIS-1, Chapter 6
Financial Management and Planning Directorate
Effective Date: AUGUST 2014

Table of Contents: **PAGE**

Reference:

(a) DoD 7000.14-R, Financial Management Regulation, Vol. 2A, October 2008.

6-1. Purpose. This chapter establishes the responsibilities of the Financial Management and Planning Directorate (Code 14).

6-2. Policy. In accordance with reference (a), the processes and procedures in this chapter establish the policy for ensuring NCIS is appropriately resourced to execute the director's strategic vision and to successfully complete its mission in support of stakeholder requirements. Abbreviations and acronyms used throughout this chapter are provided in Appendix A. Appendix B contains a glossary of financial management terms.

6-3. Cancellation. NCIS-1, Chapter 6, dated 6 December 2011, and Gen Admin 14B-0030, dated 30 April 2008, are canceled.

6-4. Chapter Sponsor. The deputy assistant directors for Planning and Evaluation (Code 14A) and Financial Plans, Programming, and Manpower (Code 14P) share joint responsibility.

6-5. Roles and Responsibilities. The Financial Management and Planning Directorate (FMPD) has two departments: Planning and Evaluation (Code 14A) and Financial Plans, Programming, and Manpower (Code 14P). Policy specific to Code 14A is provided in Appendix C. Policy specific to Code 14P is provided in Appendix D. FMPD works closely with the comptroller (who reports to the NCIS director), as well as program managers (PMs) within the directorates. The Office of the Comptroller institutes and manages a system of internal controls and maintains divisions for accounting and budget. PMs working for each of the directorate executives are responsible for carrying out the man, train, and equip functions, as well as managing performance within their directorates.

Appendix A: Abbreviations and Acronyms

AOR	area of responsibility
BSO	budget submitting office
CA	commercial activities
DCPDS	Defense Civilian Personnel Data System
EOY	End-of-Year Assessment
FMPD	Financial Management and Planning Directorate
FOQPR	Field Office Quarterly Performance Report
FOTB	Field Office Threat Brief
FOTP	Field Office Tactical Plans
GATR	Geographic Annual Threat Report
NAEPR	NCIS Annual Enterprise Performance Report
P&E	Planning and Evaluation
PDD	Program Direction Document
PM	program manager
PPMP	Program Performance Measurement Plan
PoAM	plan of action and milestones
PQPR	Program Quarterly Performance Report
MPA	Mission Performance Assessment
MPM	mission performance metric
MYA	Mid-Year Assessment
RPP	Regional Performance Plan
SLDCADA	Standard Labor Data Collection and Distribution Application
SMRDs	shore manpower requirements determinations
TFMS	Total Force Manpower System
TFMMS	Total Force Manpower Management System
TWMS	Total Workforce Management System
WBS	work breakdown structure

Appendix B: Financial Management Glossary of Terms

1. End strength (E/S). Authorized billets, as of the last day of the fiscal year (September 30). NCIS is provided an end strength target for civilian personnel. The FMPD will formulate a budget based on requirements that fund the end strength target. NCIS management is tasked to maintain a billet structure that stays within the end strength.

2. Full-time equivalent (FTE) [also known as work-year]. Number of hours expended (exclusive of overtime) divided by number of hours in the fiscal year.

3. Future Year Defense Plan (FYDP). The future year financial plan for DoD as approved by the Secretary of Defense. This is the foundation of the DoD programming system and establishes the approved force structure and financial plan for the military departments and the defense agencies' future program years.

4. Intelligence Program Budget Submission (IPBS). Annual concurrent program and budget submission from the PM of the National Intelligence Program to the Director of National Intelligence.

5. Out years. Future years (five years beyond the current budget year).

6. Planning, Programming, Budgeting, and Execution (PPBE) process. The PPBE process is used to allocate resources within the DoD. In the PPBE process, the Secretary of Defense establishes policies, strategies, and prioritized goals for the department that are used to guide resource allocation decisions that balance the guidance with fiscal constraints. It is important for PMs and their staffs to be aware of the nature and timing of each event in the PPBE process, as they will be called upon to provide critical information that could be important to program funding and success.

7. Program budget review (PBR). See Program Objectives Memorandum. PBR includes the budget year review.

8. Program manager. Collects and manages a range of assets (including manpower) to execute a particular mission area.

10. Program Objectives Memorandum (POM). The final product of the programming process within the DoD; the POM displays the resource allocation decisions of DoD components in response to, and in accordance with, Defense Planning Guidance.

11. Secretariat Review Board (SRB). Designed to extract the Secretariat financial process from the Chief of Naval Operation's POM process while still retaining a rigorous and timely review of programs and issues. The SRB objective is to produce a Secretariat budget to be presented at the same time the Services (Navy and Marine Corps) present budgets to the Secretary of the Navy. NCIS S&IA (Security and Investigative Activities) resources are funded via the SRB.

Appendix C: Planning and Evaluation

1. The Planning and Evaluation (P&E) Department is responsible for strategic and operational alignment of NCIS mission goals, objectives, and activities. Alignment is supported by the development of the NCISHQ and field planning documents, to include the Director's Strategic Vision, the Deputy Director's Strategic Goals and Focus, Program Direction Documents (PDDs), Field Office Tactical Plans (FOTPs), Field Office Threat Briefs (FOTBs), and geographical Executive Assistant Director Annual Threat Reports (GATRs), as well as the development and reporting of metrics associated with the critical activities identified in the PDDs. P&E is also responsible for maintaining effective strategic and program planning processes for NCIS and ensuring their full integration and consistency with relevant national strategies and priorities; NCIS budget and resource sponsor requirements, human resources, facilities, administration and logistics; and technical, tactical, and operational planning processes and activities.

2. P&E is responsible for conducting a variety of activities designed to assess and evaluate NCIS effectiveness, monitor and report on organization and program performance, project long-term resource and support requirements, and conduct special studies and projects related to these areas of responsibility. P&E is responsible for ensuring performance metrics are relevant to desired organizational outcomes. P&E helps to identify program performance issues for the Director, Deputy Director, programs, and field leadership. P&E also ensures evaluations are conducted to identify performance constraints and to make practical recommendations for improvement. P&E provides guidance, consultation services, counsel, and support to all NCIS organizational units to maximize the utility, relevance, and effectiveness of NCIS products. P&E facilitates the identification of long-range strategy, program plans, performance reports, and other relevant documents enabling managers to effectively meet operational requirements.

3. Strategic planning. The P&E Strategic Planning Branch is responsible for fulfilling specific strategic planning obligations on behalf of NCIS operational and support programs, ensuring NCIS' goals and objectives are comprehensive and that all field office tasks and program activities are accurately aligned with the Director's Strategic Vision.

4. The Planning Branch collaborates with program leadership to affirm the NCIS mission and vision; assists the directorates in establishing and formalizing program missions, visions, and criticality of activities in alignment with the Director's Strategic Vision; develops and maintains standardized strategic planning tools to facilitate communication throughout the agency; and demonstrates operational and support program alignment with the core capabilities established in the NCIS charter and areas of focus established in the Deputy Director's Strategic Goals and Focus. These tools include PDDs, FOTPs, Regional Performance Plans (RPPs), GATRs, and FOTBs.

5. The Planning Branch stays abreast of national and DoD directives to ensure NCIS planning documents are aligned with stakeholder requirements. Branch personnel coordinate and develop a business process that links customer requirements with NCIS capabilities.

6. Planning products. The Planning Branch is responsible for coordinating and developing the planning documents listed below.

Appendix C (Continued)
Planning and Evaluation

a. Deputy Director's Strategic Goals and Focus. This document is the organization's framework from which all other programmatic documents (PDDs, FOTPs, etc.) are developed.

b. Program Direction Document (PDD). Through working with the Program leadership, P&E produces a revised NCIS PDD every two years, based on a thorough assessment of the external and internal environment and requirements. The document sets organization direction for a two-year period. Mid-way through the cycle, an assessment is made to ensure overall agency goals and objectives remain aligned with emerging stakeholder requirements. As this is a living document, changes and modifications reflect major mission shifts in focus, as directed by NCIS stakeholders. P&E will coordinate with the operational and support program leadership to produce PDDs that describe a two-year set of objectives and performance targets for each operational and support program. P&E also ensures the quality of the plans and their consistency with the NCIS Strategic Plan, DON strategies, and national defense and intelligence strategies.

c. Field Office Threat Brief (FOTB). Field office SACs, in coordination with geographic EAD staff, are required to submit an updated FOTB every six months, timed to be briefed at the spring and fall SAC conferences. P&E initiates the process six weeks prior to the conferences. SACs submit updated FOTBs to the geographic EAD office for approval. Upon approval, FOTBs are submitted to P&E for storage on the SIPR shared drive. FOTBs are used by NCISHQ as a source of field office area of responsibility (AOR) information, including threat-based mission focus and areas of emphasis. Geographic EADs are responsible for ensuring FOTBs are updated in the format approved by the deputy director (and provided by P&E).

d. Field Office Tactical Plan (FOTP). Field office SACs, in coordination with operational program leadership and P&E, are required to submit an FOTP every two years. FOTPs are populated with field actions from the operational PDDs, as well as AOR information from the FOTB. Before the FOTPs are implemented, the geographic EADs are responsible for validating and ensuring the FOTPs meet requirements set forth in the PDDs.

e. Product dissemination. P&E will ensure that relevant products are distributed throughout the NCIS in a timely manner. This may be achieved through a variety of means, including electronic media, paper copies, and briefings. Relevant documents and finished projects will be posted on the P&E site[1] on Lighthouse, the NCIS Intranet, and on the SIPR shared drive.

7. The Planning Branch facilitates several services and products, including the following:

a. Coordinates biennial performance planning, to include the following:

(1) Reviewing national and DoD stakeholder directives.

[1] Available at: https://lighthouse.ncis.navy.mil/NCIS_Websites/01/ma/fmp/pe/Pages/default.aspx

Appendix C (Continued)
Planning and Evaluation

(2) Coordinating and facilitating the biennial process to create, produce, and present PDDs.

(3) Coordinating the FOTB update process.

b. Advises on developing policies to ensure new policies are in line with overall strategy and direction.

c. Conducts strategic reviews and develops and publishes white papers.

d. Facilitates offsite meetings/planning sessions with direct impact on planning and evaluation efforts.

e. Supports external inquiries on programs and processes, as related to planning efforts.

f. Expands current services to other customers, particularly field offices.

g. Assists planning new NCIS programs and initiatives.

h. Provides strategic and planning services (e.g., rightsizing plans, resource plans, IT plans, workforce plans, facilities plans, logistics plan, continuity of operations plan, etc.), in collaboration with other support and operational codes.

8. Evaluation. The P&E Evaluation Branch is responsible for developing, maintaining, and reporting agency, programmatic, and field mission performance metrics (MPMs) that enable the continuous monitoring and assessment of all NCIS critical activities. P&E uses strategic planning documents as a framework to facilitate innovative, meaningful, informative performance metrics from relevant subject matter experts in every facet of NCIS, via the Mission Performance Assessment (MPA) methodology. By identifying MPMs based on the critical actions and activities undertaken by the field, geographic EADs, and programs, MPA aggregates performance metrics to assess and demonstrate agency-wide performance against strategic objectives and threat-based initiatives. P&E enables a strategic decision-support capacity to key decision-makers at all levels of authority and experience. The purpose of MPA is to provide NCIS management with actionable, threat-pertinent, and performance-based decision support at the tactical, operational, and strategic level. This decision support capability enables NCIS to proactively manage critical activities and outcomes. It also allows NCIS to provide concrete qualitative and quantitative performance analysis to external budgetary and strategic stakeholders to assist in the defense or solicitation of resources.

a. MPA Requirement

(1) MPA supports aligning operational and program management activities into the Director's Strategic Vision and Deputy Director's Strategic Goals and Focus. It identifies the

Appendix C (Continued)
Planning and Evaluation

impact of agency activities and root causes of performance constraints, as well as provides sound and practical recommendations for programmatic improvements.

(2) MPA aligns directly with H.R. 2142, Government Performance & Results Act of 2010 (GPRA), a legislated strategic planning and evaluation requirement, in order to assess agency performance and improvement at the strategic, operational, and tactical levels.

b. The Evaluation Branch facilitates MPA by educating the field, programs, and agency leadership on the evaluation process and engaging relevant stakeholders and subject matter experts.

(1) Work breakdown structure. As a core component to strategic planning, P&E analysts facilitate, with senior leadership and subject matter experts in the operational and support programs and geographic EADs, identifying a program goal, mission and enterprise objectives, and critical activities to form a work breakdown structure (WBS). These elements will be defined, refined, and validated to enhance program transparency. This will better enable identifying MPMs that ultimately support a comprehensive performance assessment of the program, field, and geographic EADs. As part of the PDD/RPP/GPP development process, national strategy alignment and external stakeholder requirements will be identified.

(2) MPM and corrective action identification. Performance metrics are created around critical areas of success or failure within the process of any given critical activity. These metrics can be qualitative, quantitative, or both, depending on the activity being measured. Green, yellow, and red performance ranges are identified to qualify objective, acceptable levels of performance for each metric. Green (acceptable), yellow (acceptable but requires improvement), and red (not acceptable) indicate how well a program or field office is performing the critical activity. Corrective actions have been developed for field and program management to use when performance falls below the identified acceptable level. P&E then deploys its program management and technological and analytical expertise to either modify current tools or build practical, manageable tracking mechanisms. Standard operating procedures are developed by the relevant activity's point of contact with data to concatenate a score for each activity at the appropriate reporting period. All metrics, corrective actions, tools, and standard operating procedures are recorded in a Program Performance Measurement Plan (PPMP), which is given to the organizational unit at the end of deployment. The PPMP is to be used as an educational tool as well as a complete reference to any evaluation-related queries or issues.

(3) Management reporting. A Field Office Quarterly Performance Report (FOQPR), a Mid-Year Assessment (MYA), and an End-of-Year Assessment (EOY) are the final deliverables to programs and field offices. These reports are aggregated in the NCIS Annual Enterprise Performance Report (NAEPR) and provide proper mapping of critical activities to both agency and national strategic and threat-based initiatives. They use the balanced scorecard approach of weighing critical activities based on prominent threat and prioritized initiatives to provide the most accurate picture to management of performance and resource utilization or challenges.

Appendix C (Continued)
Planning and Evaluation

9. Activity-Based Costing Products and Services

a. Program level of effort reports. These reports demonstrate the level of effort charged to a SLDCADA (Standard Labor Data Collection and Distribution Application) activity during a specific time for a particular program. The reports are designed to illustrate resource use by level of effort within the agency programs. This style of report can be used to identify misaligned resources, justify requirements, or address mismanagement of assigned resources.

b. Project level of effort reports. These reports demonstrate the level of effort charged to a SLDCADA activity during a specific period for a particular project (e.g., Family & Sexual Violence). These reports are designed to illustrate resource use by level of effort (at every level) within the project. This style of report can be used to identify misaligned resources, justify resource requirements, or address the mismanagement of assigned resources. Project level of effort reports are specifically helpful in reporting on data calls from stakeholders with reference to level of effort against resources.

c. Attribute specific level of effort reports. The P&E Department is able to report on NCIS enterprise level of effort based on several specific activity attributes (e.g., Charter Mission Functions, MPA Critical Activities).

d. Cost of the agency reports. These reports demonstrate the cost of the agency (at any level) from a resource perspective (allocated dollars), from an activity perspective (expended dollars), and from an output perspective (e.g., cost per case, cost per case category).

10. P&E Program Management

a. Program management support. The P&E Department is responsible for supporting NCIS PMs through subject matter expertise, consultation, and products and services.

b. Value of program management support

(1) P&E provides an environment for PMs to address mission priorities in a more efficient and effective manner.

(2) P&E provides core PM subject matter expertise to NCIS leadership as a recurring and continuously evolving resource.

(3) P&E provides a force multiplier to PMs in areas that require PM subject matter expertise, guidance, and products, as needed.

c. Program management products & services. P&E will provide PM products and services to PMs on a recurring and as-needed basis. These products and services include the following:

Appendix C (Continued)
Planning and Evaluation

(1) Leadership Development Program. P&E will provide tailored presentations and instruction on PM subject areas as required for professional development (SSA, ASAC, etc.).

(2) Program management reference products. P&E will produce, disseminate, and update a PM resource product for NCIS leadership, which will contain useful information and guidance on PM subjects that are relevant to NCIS' mission profile and roles and responsibilities.

(3) Program engagement. P&E will proactively engage with PMs to gain better insight and understanding of the roles and responsibilities of NCIS PMs. This engagement will assist P&E in tailoring PM support services and products to individual program needs.

(4) PM subject matter expertise. P&E will provide proactive PM subject matter expertise to NCIS leadership that is tailored to the needs of the agency. P&E will continue the professional development of its staff in PM areas of knowledge.

(5) Project planning & execution support services. As PMs take on and start new projects, P&E will provide, as needed, project planning and execution support. P&E will facilitate the following types of support, as needed:

(a) Strategy development. Develop realistic and achievable mission-focused strategies that are properly prioritized and aligned with national-, Service-, and agency-level mission priorities and requirements.

(b) Project plan of action & milestones (PoAM) development: Develop PoAMs to aid programs in planning and executing specific projects within their mission portfolios.

(c) Process mapping. Help PMs identify and map business processes and producing appropriate products for program use. This service will provide better understanding and clarity of NCIS business processes within the enterprise, assist with identifying inefficient or redundant processes, and serve as a driver for PMs to improve process effectiveness and overall program performance and efficiency.

(d) Rightsizing. Work closely with NCIS leadership to develop, document, validate, and establish an agency rightsizing methodology that will meet PM needs of placing the right person in the right place at the right time.

Appendix D: Financial Plans, Programming, and Manpower

1. The FMPD is responsible for formulating a five-year strategic resource program. The strategic program is developed collaboratively with NCIS PMs. This five-year plan will be reviewed and updated each year to incorporate internal and external environmental changes.

2. The FMPD is responsible for coordinating and facilitating DON budget year requirements with the comptroller, P&E, and NCIS PMs for the Congressional Joint Budget Justification and Congressional Joint Book. FMPD will facilitate DON execution year performance requirements, as those requirements dovetail with resourcing documents. FMPD will ensure performance issues are first coordinated with P&E personnel to ensure consistency in external performance reporting. FMPD will ensure final copies of performance products are provided to P&E.

3. The FMPD will work collaboratively with PMs and P&E to develop organizational financial requirements and ensure requirements are within guidance provided by the DON and P&E. Necessary resources and materiel requests will be solicited from support organizations and converted into dollar requirements. Additionally, alternative solutions will be explored and recommended as appropriate. The FMPD will work with the Communications Directorate, P&E, and PMs to assist in ensuring consistency in reporting (financial/performance) and to promote and proliferate the mission performance success and needs (risk identification) to NCIS stakeholders. The FMPD will ensure all financial documents are submitted to the resource sponsors on a timely basis and facilitate a review process for final decisions by the Director, when required. The FMPD is responsible for following the program request through the external oversight process, keeping senior management advised of the actions taken.

a. Resource Review Board. The FMPD will develop, schedule, and administer a resource review process for resourcing decisions affecting out-year funding. Participation will be at the PM level, with final decisions approved by the Deputy Director (or designee). The board will convene at scheduled times throughout the year to address the following issues:

(1) Strategic guidance (as summarized by Code 14A) and the Director's priorities (and related issues).

(2) Billet change requests (requests approved at the Code 14 level and those requiring board recommendations (e.g., cross-cutting force structure changes, changes in priority program billet structure).

(3) Resource changes or reviews.

(4) Program unfunded requirements/decrement list.

b. Resource tracking. The FMPD will develop and maintain standard resource trackers for each program cycle to facilitate retrieving historical resourcing data. The retained information will include ease of access electronic folders containing resource trackers for each funding stream as well as the source documents causing changes to resources.

Appendix D (Continued)
Financial Plans, Programming, and Manpower

4. Manpower. FMPD is responsible for billet structure. Billet change requests must be approved by the PM and appropriate level of leadership in the directorate before forwarding to FMPD. Other billet change requests will be consolidated for review and approval by the Deputy Director. All changes will be documented and a record retained for the appropriate retention period. Once requests are approved, Total Force Manpower System (TFMS) packets will be prepared to update the NCIS official manning document and TWMS. FMPD is the focal point for all manpower actions. Components of manpower management include total force manpower management, manning, manpower, resourcing, human resources liaison, and civilian and military workforce. Manpower will be included in the POM and performance review input cycles to provide guidance on determining the quantity and quality of billets required, and the planning, programming, budgeting, and execution system phases of activity management.

a. FMPD will perform the following functions:

(1) Provide analytical and advisory support to programs across NCIS. Provide recommendations to EADs, Assistant Directors, and PMs on best use of available resources, strategies, and techniques for executing requirements.

(2) Evaluate organizational structures, reporting relationships, and supervisor and worker ratios to recommend best mix of skill levels required in concert with human resources and civilian community management. Evaluate and indicate concurrence and validation of request for personnel action for civilian personnel requirements (to ensure billets exist and are funded).

(3) Implement shore manpower requirements determinations (SMRDs) or other Navy-wide approved requirements determination studies, including interface with claimant and budget submitting office (BSO), OPNAV, and officer and enlisted community managers to complete implementation actions. Develop rationale and supporting documentation for new or adjusted requirements for validation.

(4) Manage the Total Force Manpower Management System (TFMMS), which includes documenting requirements correctly, as well as realigning, transferring, reducing, and changing billet requirements and funding authorizations to support mission-driven program changes.

(5) Support higher authority manpower information and data calls in response to BSO, OPNAV, POM, and/or specific issue data calls, studies, evaluations, reviews, and/or total force manpower needs.

(6) Track enlisted and officer personnel assignments to ensure validity of activity manpower documents.

(7) Participate, as needed, to assist with liaison to detailers, placement officers and community managers, enlisted placement management center, and manning control authorities to gain fill of authorized billets and Navy manning plan.

Appendix D (Continued)
Financial Plans, Programming, and Manpower

(8) Respond to BSO-level direction to identify and provide military personnel in response to augmentation requirements. Analyze current military billet structure and manning across field offices and NCISHQ to determine the best office or program source for tasking. Monitor execution of augmentation and track distribution of augmentation taskers.

(9) Coordinate priority manning submissions and tracking of status for implementation.

(10) Review and provide data for staffing plans, projections, demographics, and trends.

(11) Identify and monitor military and civilian personnel end strength authorizations through the programming and budget cycles. Recommend and distribute available civilian end strength within the appropriate databases (TWMS) to meet operational requirements; monitor implementation of resource distribution compared to operational requirements and plans.

(12) Coordinate with planners and PMs for requirements development and resource requirement profiles and execution results for use in the budget, POM and annual certified obligations processes.

(13) Coordinate with Code 10 regarding civilian personnel staffing, commercial activities (CA) study implementation (CA is limited for NCIS; most billets are exempt) hiring freezes, reductions in force, etc. Perform reconciliation and maintenance reviews with human resources personnel of the human resources/Defense Civilian Personnel Data System (DCPDS) to ensure accuracy of personnel data fields and corrective maintenance is identified.

b. FMPD will also prepare periodic reports on human capital status, in collaboration with other NCIS activities, for NCIS leadership and field offices and Headquarters activities.

5. Total Workforce Management System (TWMS). FMPD is responsible for managing the NCIS TWMS. The FMPD TWMS program manager will perform the following functions:

(1) Assist designated TWMS contacts within the directorates in troubleshooting issues that cannot be resolved by the TWMS Help Desk.

(2) Coordinate and prioritize agency requests with the TWMS program management staff.

(3) Develop and edit new and existing TWMS training materials.

(4) Provide TWMS training.

(5) Assist with TWMS reconciliation requirements (e.g., with Payroll, Manpower).

NCIS-1, CHAPTER 7
TITLE: SUPPLY, PROPERTY, AND EQUIPMENT
POC: CODE 11B
DATE: NOV 08

7-1. GENERAL

7-1.1. This chapter promulgates policy and procedures for ordering, receiving, and shipping supplies, ammunition, or equipment and establishes property accountability and equipment management processes.

7-1.2. The Naval Criminal Investigative Service Headquarters (NCISHQ) and each affiliated field office is responsible for procuring supplies, equipment, and services for their cognizant activities, within their given authority, using the Navy supply system, open market, or Department of Defense (DoD) E-mall. NCISHQ will adhere to all established rules and procedures contained in the Naval Supply Systems Command (NAVSUP) P-485 Manual, Volume III, Ashore Supply, the Federal Acquisition Regulation (FAR), the Defense Federal Acquisition Regulation System (DFARS), Procedures, Guidance, and Information (PGI), (a companion resource to the DFARS that is available electronically at http://www.acq.osd.mil/dpap/dars/index.htm), the Navy Acquisition Procedures Supplement (NAPS), NAVSUPINST 4200 Series, SECNAVINST 7320.10A, Defense Property Accountability System (DPAS), DPAS User Manual Release 16.6.00 series, and local supply activity instructions and notices.

Due to the expansive area covered by the various field offices, decentralization of supply activities and self-reliance is stressed in order to provide as timely and local support as possible.

7-1.3. Definitions

a. Consumables. Administrative and housekeeping items, common tools, paints, cognizance symbol forms, or other items not specifically defined as equipment or plant property.

b. Minor Property. Equipment having a unit cost of less than $100,000 and more than $5,000.

c. Sub-Minor Property. Equipment having a unit cost of less than $5,000. These items are usually portable or pilferable and warrant management attention to safeguard

the assets and to insure proper maintenance is performed. Examples include calculators, typewriters, non-NMCI personal computers-printers, shredders, owned copiers, transcribers, binoculars, televisions, VCR's, cameras and video equipment.

d. Plant Property. Navy-owned real property of a capital nature having an acquisition cost of $100,000 or more. More extensively defined in NAVCOMPT Volume III 036004, plant property items are divided into four classes: Class (1) - Land, Class (2) - Buildings, Structures, and Utilities, Class (3) - Equipment Other than Industrial Plant Equipment, and Class (4) - Industrial Plant Equipment.

(b)(7)(E)

f. Expendable Investigative Supplies. Consumable items used for crime scene investigations.

g. Leased Property. Equipment that is leased from a commercial activity and requires maintenance and periodic contracting services, such as copiers and vehicles.

h. Ammunition. Small arms rounds that are allocated by Naval Sea Systems Command (NAVSEA) for use in NCIS approved weapons. Ammunition requires special handling, reporting and management using the Retail Ordnance Logistics Management System (ROLMS) or Ordnance Information System (OIS).

i. IT Equipment. Telecommunication, cellular phones, pagers, beepers, word processing, personal computers, wide area network systems (WANS), local area network systems (LANS) or other information technology (IT) equipment.

7-2. REQUISITIONING PROCEDURES

7-2.1. Each NCIS field office shall provide supply support and guidance for their subordinate activities and ensure compliance with supply procedures and instructions.

a. General Supplies. Office supplies, standard forms and equipment normally available in the Navy supply system will be procured directly by the cognizant NCIS field office.

b. The NCIS Supply Branch, NCIS Code 11B2 maintains a stock of criminal investigative supplies, and NCIS forms not available through the Navy supply system or on the NCISnet. A listing of approved criminal investigative supplies is maintained on the NCISnet Acquisition and Logistics website at http://infoweb/agency/deptwebsites/acqlog/al-index.html. Supplies carried in stock are issued at no charge to the requesting component.

c. Unique or high cost items, such as investigative equipment, investigative consumables and information technology, will be procured centrally by NCISHQ for distribution to field offices.

7-2.2. Requisitions for supplies, equipment and services will be processed according to NAVSUP P-485 Manual, Vol. III (Ashore Supply), NAVSUP P-437 MILSTRIP/MILSTRAP and local supply activity instructions or notices.

7-2.3. The following guidelines indicate proper sources for procuring various types of supplies and services:

a. Consumables. These items are available through Defense Logistics Agency (DLA), DoD E-mall, DAPS, and local self-service stores or from the nearest Naval supply activity. Procedures for procurement of consumables vary slightly from one location to another. Information on local procedures may be obtained by contacting the self-service store in your area. Consumables not readily available through the above listed sources or self-service stores can be requested through the parent NCIS field office for procurement action. The following sites include further ordering information, stock numbers, nomenclatures and other useful information:

(1) www.dlis.dla.mil/Fedlog;

(2) http://www.emall.dla.mil;

(3) http://forms.daps.dla.mil;

(4) https://www.onetouch.navy.mil/ots/jsp/LoginPage.jsp;

(5) http://www.cnrsw.navy.mil/hrocnrsw/forms1.htm, and

(6) https://nll1.ahf.nmci.navy.mil.

b. Technical and Investigative Equipment. Requirements should be communicated to the nearest NCIS field office technical services detachment (TSD). Informal discussion with TSD personnel about specific applications, the type of equipment available and its capabilities and limitations is strongly encouraged. NCIS Code 24B Field Services Support will provide second echelon support to the detachment as required and will have cognizance in procuring equipment not already available.

c. Investigative Supplies. Requests for criminal investigative supplies should be developed using the list provided at the NCISnet Acquisition and Logistics website. Requests should be sent to NCIS Code 11B2 via e-mail, telephone, or facsimile, with a copy to the parent NCIS field office crime scene specialist indicating the item description, vendor code, quantity requested. “Restricted” supplies can only be ordered by forensic consultants or a field office crime scene specialist. Orders will ship within 72

hours. NCIS Code 11B2 will notify the customer via e-mail when the shipment is sent. Back ordered items will be automatically shipped when available.

d. Leather Gear. Holsters, pouches and handcuff cases are procured, stored and issued by NCIS Code 11B.

e. Ammunition Requisitioned via Military Standard Requisitioning and Issue Procedures (MILSTRIP). NCIS Codes 11B will procure ammunition for offices in the National Capital Region. All others will coordinate procurement actions through the responsible field office. The following site provides MILSTRIP guidance and definition: https://www.drms.dla.mil/rtd03/milstrip.htm.

f. Minor Property, Equipment and Furniture. Requirements for minor property equipment, and furniture with an acquisition cost less than $100,000 will be coordinated through the parent NCIS field office. Procurement of technical and/or investigative equipment within this category must be coordinated with NCIS Code 24B or field office TSD.

g. Plant Property. When a plant property requirement exists, NCIS Code 11B will coordinate all procurement actions and provide guidance for the establishment of a plant property record.

h. Restricted Procurements or Items Requiring Special Approval. All purchasing activities are restricted or prohibited from procuring the items listed in NAVSUPINST 4200.85C, enclosure (3), without acquiring special approval from the cognizant department at NCISHQ. Examples of these items include:

(1) Membership Dues. Memberships must be in the agency name. The membership must contribute to the fulfillment of the mission of the activity or agency (refer to NCIS-1, Chapter 42 for specific guidance on memberships);

(2) Personal Services. Procurement of personal services is not authorized;

(3) IT Equipment. The lease, purchase or maintenance of IT equipment must be coordinated with and approved by NCIS Code 15, Information Technology;

(4) Reprographic Equipment. Requests for copying equipment which produces 70 or more copies a minute, or for which the purchase price exceeds $25,000 requiring Operations Navy (OPN) funding, must be submitted to the supporting local DAPS office prior to lease or purchase. Requisitioners are responsible for providing supporting documentation for consideration by DAPS to include a cost-benefit analysis statement, which determines if it is more economical to purchase or lease a copier, and must consider the cost of copier maintenance. NCIS field offices must submit NCIS Form 4238 to NCIS Code 14, Financial Management and Planning Directorate for approval of funding. NCIS Form 4238 must provide the DAPS purchase approval number,

manufacturer and model of equipment and a justification for purchases $25,000 and over, which require OPN funding;

(5) Telecommunication Equipment. Submit requirements to NCIS Code 15 for review and approval; and

(6) Photographic and Video Equipment. Submit all requests for equipment in this category to the NCIS field office TSD. Additional support will be provided by NCIS Code 24B.

i. Repairs. Prior to initiating maintenance or repair action funding documents, NCIS field offices should ensure IT items, technical equipment, vehicles, etc, are not covered under manufacturer's warranty or existing maintenance contracts established by NCISHQ.

j. State and Local Taxes. Purchases and property of the Federal Government are exempt or immune from state and local taxation in accordance with FAR subpart 29.3. Evidence needed to establish exemption from state and local taxes depends on the grounds for exemption claimed, the parties to the transaction, and the requirements of the taxing jurisdiction. Evidence supporting tax exemptions may include the following:

(1) A copy of the contract or relevant portion;

(2) Copies of purchase orders, shipping documents, paid or acknowledged invoices, or similar documents that identify NCISHQ as the buyer;

(3) A U.S. Tax Exemption Certificate is available from Code 11B1 for vendor use; and

(4) A state or local form indicating that the supplies or services are for the exclusive use of the United States. The form is provided by and maintained by the requesting state tax office.

7-3. MATERIAL RECEIPTS

7-3.1. General**.** Expeditious and accurate processing of documentation regarding material and services received is incumbent upon all concerned. The timely payment of invoices is imperative and is required in order to qualify for discounts under the Prompt Payment Act, and to avoid unnecessary penalties.

7-3.2. Procedures. Verify that NCIS gets what is ordered and pays for only the items received. The following guidelines are provided to ensure proper receipt processing is performed.

a. Upon receipt of material or services requisitioned or purchased by NCISHQ or NCIS field offices, the receiving activity will immediately inspect the contents for quality

and quantity of purchased material, indicate whether the order is complete, or a partial delivery, sign and date the packing slip or other shipping documents. Discrepancies in receipt must be noted and conveyed to the NCIS purchasing agent or buyer.

b. Notify the purchasing agent or buyer via e-mail to initiate a tracer action when a shipment is not received within two weeks of the estimated delivery date.

c. Receipt documents for items purchased by NCISHQ for direct delivery to the NCIS activity must be certified and forwarded to NCIS Code 11B for processing. Packing slips and receipts must be forwarded to NCIS Code 11B within five working days of receipt.

d. Material received without a packing slip must have a dummy receipt document prepared and forwarded. The dummy receipt should include the following information:

(1) Purchase order/requisition number

(2) Manufacturer

(3) Model number

(4) Serial number

(5) Quantity

(6) Nomenclature (i.e., printer ribbons, toner cartridges)

(7) Date of receipt

(8) Name of individual accepting receipt of supplies

(9) Other identifying information that will assist the ordering activity in processing the invoice.

e. All NCIS activities should retain copies of signed receipt documents in a completed requisition file for proof of receipt and further inquiries.

7-4. PROPERTY, PLANT AND EQUIPMENT

7-4.1. Control and Accountability

a. Responsibility. The control of property, plant and equipment items is the responsibility of each NCIS field office, and cognizant NCISHQ codes. However, oversight of all properties is managed by Code 11B2 - UIC 63285.

b. Inventory. The DPAS provides an automated means of accounting for and reporting of assets. The oversight of inventory and accountable management of those

items used, but not consumed, is included in this system, such items as office equipment, industrial plant equipment, material handling equipment are accountable property, IT equipment and software, Government Furnished Property (GFP), and other types of assets including leases and military equipment. NAVCRIMINVSERVINST 5000.64 Defense Property Accountability System (DPAS) Management and Administration, provides guidance on the management and accountability of DoD property under the control of the Director, NCIS in compliance with SECNAVINST 7320.10A and other applicable DoD instructions.

7-5. MATERIAL EXPENDITURES

7-5.1. General. Each NCIS activity is responsible for ensuring material expenditures are documented and have proper audit trails to verify adequate control and accountability, and for validating legitimate use of government funds and assets.

7-5.2. Procedures

a. Processing. Material expenditures will be expeditiously processed per the expenditure procedures outlined by the NAVSUP P-485 Manual, Vol. III, Chapter 5. Material expenditures must be accurately recorded on an applicable disposition document, normally DD Form 1149, DD Form 200, or a locally directed turn-in document. Locally assigned expenditure document numbers should be used to properly cross reference the expenditure transaction from the document to applicable property records. Expenditure files must be maintained to show proper accountability and audit trails.

b. Surveys. The term "survey" refers to the procedures for determining the cause of gains, losses, or damage to government property. Also, it determines the procedure for establishing personal responsibility (if any) and documenting necessary inventory adjustments to stock records. A survey is required when loss, damage, or destruction of Government property involves death or injury or property value exceeds $200 or there is a possible claim against the government. The form used for survey is the Financial Liability Investigation of Property Loss, DD Form 200. The purpose of the form is to report the facts and circumstances supporting the assessment of financial charges for the loss, damage, or destruction of DOD-controlled property. The NAVSUPINST 4440.115 series provides procedures for processing the DD Form 200. Surveys of lost, stolen or damaged property will be expended on a DD Form 200 per NAVSUP VOL II.

c. Disposals. Serviceable property estimated to be worth $500.00 or more must not be turned over to a property disposal activity or returned to NCISHQ without prior authorization from NCIS Code 11B. Technical equipment will not be disposed of without prior approval of NCIS Code 24B. Requests for disposition approval should be forwarded via e-mail or letter stating status of equipment requiring disposition. Transfer of excess equipment to other NCIS or U.S. Government activities is preferable to disposal at the local Defense Reutilization and Marketing Service (DRMS). For more information go to: http://www.drms.dla.mil/.

7-6. SUPPLY FORMS

7-6.1. Listing. Several of the more commonly used supply forms are listed below. Details to complete these forms are in the applicable NAVSUP and NAVCOMPT manual(s) annotated below each form. Both the NAVSUP and NAVCOMPT manuals should be maintained at each NCIS field office and local supply activities. Guidance and assistance to determine the correct forms to use, as well as detailed information necessary to complete each form, may be obtained by contacting the NCIS Field Office Manager or the Customer Service Officer of the local supply activity. Most forms are available on-line in PDF format at http://www.dtic.mil/whs/directives/infomgt/forms/formsprogram.htm.

a. NCISHQ Form 4238 Request for Supplies or Services. This form can be found on the NCISnet. Form 4238 is used to initiate a purchase for products and, or services. The website address to download NCISHQ Form 4238 is http://infoweb.ncis.navy.mil/downloads-forms.html.

b. DD Form 1348 Single Line Item Requisition System Document. This form is used to requisition national stock numbered items from government supply activities. Refer to NAVSUP P-437 MILSTRIP/MILSTRAP Operating Procedure Manual or your local supply activity. The website address to download DD Form 1348 is http://www.dtic.mil/whs/directives/infomgt/forms/forminfo/forminfopage493.html.

c. NAVCOMPT Form 2275 Order for Work and Services. The NAVCOMPT Form 2275 is used for requisitioning work and/or services from any activity or organization of the U.S. Government. This form is prepared and signed by the accounting division. The website address to download NAVCOMPT Form 2275 is https://navalforms.daps.dla.mil/formsDir/_NAVCOMPT_2275_4230.pdf.

d. NAVCOMPT Form 2276 Request for Contractual Procurement. The Request for Contractual Procurement (RCP) is utilized for requesting contractual procurement or local purchase of material or service. This form is prepared and signed by the accounting Division. The person requiring the contractual procurement must initiate the NCIS Form 4238. The website address to download NAVCOMPT Form 2276 is https://navalforms.daps.dla.mil/formsDir/_NAVCOMPT_2276__6C__3204.pdf.

e. DD Form 1149 Requisition and Invoice/Shipping Document. This form is used to requisition non-stock numbered items from government activities. It is also the primary document used for shipments between government activities. The website address to download DD Form 1149 is http://www.dtic.mil/whs/directives/infomgt/forms/forminfo/forminfopage326.html.

f. DD Form 1155 Purchase/Delivery Order. Procurement offices having contracting authority to procure supplies or services from commercial and government sources use

this form. The website address to download DD Form 1155 is http://www.dtic.mil/whs/directives/infomgt/forms/forminfo/forminfopage329.html.

g. DD Form 200 Financial Liability Investigation of Property Loss. This form is used to report the obsolescence, non-serviceable, loss, destruction, etc., of property. Refer to NAVSUP P-485. The website address to download DD Form 200 website address is http://www.dtic.mil/whs/directives/infomgt/forms/forminfo/forminfopage43.html.

h. DD Form 1348-1 DoD Single Line Item Release/Receipt Document. This form is used for the expenditure or disposal of government property. Refer to the NAVSUP Manual Volume II and the local DRMO for instructions. The website address to download DD Form 1348-1 is http://www.dtic.mil/whs/directives/infomgt/forms/forminfo/forminfopage495.html.

CHAPTER: 8
TITLE: WORK HOUR REPORTING
POC: CODE 14
DATE: MAR 10

8-1. BACKGROUND

8-1.1. The Naval Criminal Investigative Service (NCIS) uses the Department of the Navy standard timekeeping system to capture and report on hours worked, to request and approve leave, and to request and approve overtime. The Standard Labor Data Collection and Distribution Application (SLDCADA) is an automated web-based application which has been distributed for use by individual employees at all NCIS locations worldwide.

8-1.2. SLDCADA also captures reporting on labor distribution codes (commonly referred to as operational or OP codes) as a means of identifying the level of effort expended within each of several operational and administrative work streams. The resulting data can be queried via the NCIS Dashboard by NCIS headquarters (HQ) and field managers and is used for agency policy and programmatic decisions where labor hours may be a factor. It is imperative that all NCIS employees diligently and correctly enter the appropriate labor hours to ensure they are paid properly, to enable NCIS to report on the level of work effort in the various mission areas and to justify future agency budget requests.

8-1.3. Background information on SLDCADA and detailed user information is contained in several guides posted on the NCIS Infoweb site. These guides may be accessed through the following link: NCISnet-GUIDELINES AND REFERENCE [NCIS Manuals and User Guides]. Detailed information on work schedule options, overtime and compensatory time policies, and alternative worksites is found in NCIS Manual 1, Chapter 15.

8-2. DEFINITIONS

8-2.1. Functions: The grouping of program activities (e.g., investigations, operations, adjudication, polygraphs, etc.) which are performed by NCIS employees.

8-2.2. NCIS Dashboard: The web application which is used to query multiple NCIS databases. This is sometimes referred to as the “Labor Dashboard” when querying work hour data.

8-2.3. Training, Leave and Travel Hours: Work hours designated to leave, travel, physical fitness, and training received.

8-2.4. Operational Code (OP code): The two letter and two digit code in SLDCADA representing the type of work performed by the employee.

8-2.5. Productive Hours: Work hours performed in furtherance of the primary and supporting NCIS mission areas.

8-2.6. Programs: The overarching areas which make up the total NCIS mission. They are combating terrorism, counterintelligence, criminal investigations and law enforcement, cyber, intelligence and information sharing, operations support and management and administration.

8-2.7. Type Hour Code (THC): A two letter code that refers to the type of time being recorded. Type hour codes are used to describe working hours or leave hours. Two examples are RG for regular hours and LA for annual leave.

8-2.8. Work year: One work year is equivalent to 2,087 hours per fiscal or calendar year. A work year is comprised of all productive, training, leave and travel hours. For program planning purposes, Code 14 has defined a productive work year as 1,942 hours for special agents and 1,643 hours for non-agent personnel. Training, leave and travel hours are 595 for special agents and 444 for non-agent personnel per work year.

8-3. RESPONSIBILITIES

8-3.1. All NCIS employees (civilian, military, reservist, intern, and detailees from other agencies) are required to enter hours worked into SLDCADA. Contractors are not required to enter data into SLDCADA.

8-3.2. Supervisors are responsible for reviewing and certifying the accuracy of their employees' biweekly time and attendance reports.

8-3.3. The Financial Management and Planning Directorate (Code 14) is responsible for:

a. Managing the architecture by which work hours are collected and used; and,

b. Maintaining NCIS policy on the process; and,

c. Approving the creation, revision or deletion of OP codes; and,

d. Evaluating the efficiency and effectiveness of the work hour collection process; and,

e. Implementing processes to ensure data quality. At a minimum, Code 14 will review the records with default (DFLT) hours or unknown employees and ensure the records are corrected by the end of each fiscal year.

8-3.4. The Human Resource Directorate, Personnel Operations and Services Department (Code 10A):

a. Enters the master list of OP codes into SLDCADA; and,

b. Provides guidance on SLDCADA operations that impact the time and attendance (T&A) process; and,

c. Reassigns in SLDCADA those personnel transferring to another field office or HQ to their new office and supervisor tree based upon receipt of a personnel status report (PSR (GAIN)) or email.

8-3.5. The Information Technology Directorate (Code 15):

a. Merges data from SLDCADA into the Labor Dashboard after each pay period; and,

b. Creates data queries and reports which allow users to access work hour data.

8-3.6. Special agents in charge (SACs) and deputy assistant directors (DADs) are responsible for ensuring new hires are properly indoctrinated on the work hour reporting system and process.

8-3.7. The NCIS Inspector General will review the certification of time and attendance reporting as part of the inspection process.

8-3.8. Timekeepers are responsible for entering assigned military, intern, and reserve personnel, into SLDCADA and for performing required biweekly internal controls. Civilian personnel are automatically entered into SLDCADA from the Defense Civilian Personnel Data System (DCPDS) when hired.

8-3.9. Program direction DADs must provide the proper OP code to use when announcing employees have been selected for training, deployments or other special evolutions.

8-4. GENERAL RULES

8-4.1. Employees must select the OP code which reflects the work performed (e.g., port visit support, training received, or death investigation, etc.). Hours should be tied to operational missions whenever possible. For example, special agents should use RC01 (Crimes Against Persons Investigations) vice AD01 (General Administration) to record time spent organizing case files.

8-4.2. The approved OP codes will be used by NCIS employees to enter labor hours for work performed. Labor hours attributed to OP codes will reflect both regular, Law Enforcement Availability Pay (LEAP), compensatory time, and overtime work performed.

8-4.3. Supervisors and managers (e.g., assistant special agents in charge (ASACs) and HQ program direction personnel) must use the Management/Supervision codes (e.g., CT20, FC20 or

RC20) for their assigned mission area rather than the AD12 (General Management). HQ desk officers must use the OP codes associated with the type of cases being supported (e.g., FC01 (CI Investigations), CT02 (CT Operations), or EC02 (Procurement Fraud Investigations)).

8-4.4. Program support assistants must use the Administrative/Clerical codes (e.g., CT25, FC25 or RC25) for their assigned mission area rather than AD01 (General Administration).

8-4.5. Special agents must use AD16 (Travel) when traveling more than 4 hours during the regular work day. This will ensure the day is not counted as a full work day in computing LEAP hours. Travel of less than 4 hours during regular hours, or any travel recorded as LEAP, must be associated with the type of cases being supported (e.g., OP codes FC01 (CI Investigations), CT02 (CT Operations), or EC02 (Procurement Fraud Investigations)).

8-4.6. Compensatory time for travel earned must be recorded using the type hour code CB and the OP code associated with the type of cases being supported (e.g., FC01 (CI Investigations), CT02 (CT Operations), or EC02 (Procurement Fraud Investigations)).

8-4.7. Special agents afloat should use OP code CT03 (Port Visit Support) when deployed and not conducting operations or investigations covered by a more specific OP code.

8-4.8. OP codes are assigned as follows:

OP codes starting with:

AD – Management and administration
BI – Biometrics
CC – Cyber activities
CF – Adjudications
CM – TSCM program
CT – Combating terrorism program
DI – Intelligence and information sharing activities
EC – Fraud and economic crime program
FC – Counterintelligence program
FD – Forensic consultants
IF – Information systems support
PE – Polygraph
PL – IG activities
PS – Navy security program
RC – Criminal investigations and law enforcement program (reduce crime)
SE – STAAT activities
TE – Technical services
TR – Training

OP codes ending with:

15 – Contingency deployments such as Iraq and Afghanistan

20 – Supervision and management (including program management)
25 – Administrative and clerical support

8-4.9. Leave: All leave will be recorded using the OP code LVLV. Employees will use the THC to indicate the type of leave taken. Some examples are:

LA – Annual leave
LH – Holiday leave
LS – Sick leave
LY – Time off award
CT – Compensatory time taken
CF – Travel compensatory time taken

8-4.10. Training Received: Record time spent in training (formal courses, in-service training, firearms qualifications) using TR12 (Training Received). Special agents and military personnel record time expended on physical fitness training as TR30 (Physical Fitness).

8-4.11. Deployed personnel: Due to complications accessing SLDCADA while deployed, plus difficulties accurately capturing and maintaining deployed supervisory hierarchies, deployed personnel will provide their supervisor and timekeeper in their permanent duty assignment (field office or HQ code) their hours worked. Permanent timekeepers are responsible for accurately recording time and attendance records and work hour data for their respective deployed personnel. They are also responsible for recording time and attendance for those personnel without access to SLDCADA. Permanent supervisors are responsible for certifying time and attendance records for their deployed personnel and they are encouraged to communicate with deployed personnel and supervisors, as required, to perform those certifications.

8-4.12. Problems with SLDCADA should be addressed to the timekeeper, who will attempt to resolve problems at the local level. If necessary, the timekeeper will refer issues related to the information technology system supporting SLDCADA to Code 15 via Remedy. The timekeeper will refer T&A questions to Code 10A.

8-5. CREATING/AMENDING/DELETING OPERATIONAL CODES

8-5.1. The OP codes within SLDCADA can be created, amended, or deleted using the process described below. This process will be used to ensure uniformity and that the programmatic imperative for amending, deleting, or creating codes is appropriately matched with the strategic policies of the agency.

8-5.2. Any office or code within NCIS can propose the creation, amendment, or deletion of an OP code. The following guidelines should be considered when preparing the proposal. Newly proposed OP codes must:

a. Relate to a primary NCIS mission area or support a primary NCIS mission area.

b. Tie to a programmatic function.

c. Generally involve more than five work years of effort. There should not be multiple OP codes that are used by a small number of employees.

d. Respond to a stakeholder requirement or are necessary to evaluate a program.

8-5-3. The proposal for creation/amendment/deletion of an OP code should be written in standard memorandum format and be submitted to Code 14 via the tasker system. The memorandum should contain the following:

a. The (proposed/amended/deleted) OP code; and,

b. Program sponsor; and,

c. Functional area under the program; and,

d. OP code definition; and,

e. Internal/external stakeholder for the OP code; and,

f. Approximate number of employees that will be affected by or use the proposed OP code; and,

g. Justification to include:

1) How the proposed OP codes relates to the NCIS mission; and,

2) How the proposed OP code will assist the program; and,

3) The deficiency or efficiency being addressed by the proposal.

8-5.4. The executive assistant directors (EAD)/assistant directors (AD) for the program area the OP code falls under will endorse the proposal. The memorandum and EAD/AD endorsement will be forwarded to EAD, Code 14.

8-5.5. The EAD, Code 14 will approve/disapprove the proposal. Resulting changes will be forwarded to Code 10A to update the OP code listing in SLDCADA and to Code 15 to update the Labor Dashboard in Business Objects.

8-5.6. Code 14 will make the appropriate changes in Appendix 1 of NCIS-1, Chapter 8, and disseminate changes via a General Administrative message.

APPENDIX (1): SLDCADA CODES

Frequently Used Codes					
Code		**Program**	**Function**	**Case Category**	**Description**
LVLV	Leave (All Categories)	Other	Leave	N/A	Civilian and military employees in conjunction with the type hour code (THC) corresponding to the type of leave taken (All).
AD16	Travel Time (SAs Only)	Other	Travel	N/A	Hours spent by 1811s on travel. Hours coded as AD16 do not count as regular hours in the calculation of the LEAP substantial hours requirement (civilian 1811s only).
TR12	Training Received	Other	Training	N/A	For all employees to document time spent attending training.
TR30	Physical Fitness	Other	Training	N/A	Special agents and military personnel to document time spent conducting physical fitness assessments and participating in physical fitness programs.
DFLT	Temporary DAL Code (Missing)	Other	N/A	N/A	Automatically assigned by SLDCADA when no entry is made for an employee's biweekly report.
Administrative Codes					
Code		**Program**	**Function**	**Case Category**	**Description**
AD01	General Administration	Management and Administration	Administration	N/A	To document general administrative tasks that cannot be associated with any other operational code (All).
AD02	Financial Management	Management and Administration	Financial Management	N/A	Managing financial resources such as EEE (HQ/field).
AD03	Legal Staff	Management and Administration	Legal	N/A	Legal support and FOIA reviews (Code 00L).
AD04	Public/Legislative Affairs	Management and Administration	Communications	N/A	Coordinating public affairs and legislative issues (HQ/field).

AD05	Procurement/Supply Acquisition/Logistics	Management and Administration	Acquisition and Logistics	N/A	Procuring supplies, maintaining vehicles and administering contracts (HQ/field).
AD06	Facilities	Management and Administration	Facilities	N/A	Maintaining NCIS facilities (HQ/field).
AD07	Security	Management and Administration	Security	N/A	Administering information and personnel security programs for NCIS activities (HQ/field).
AD09	Record Storage and Management	Management and Administration	Administration	N/A	HQ personnel to record hours associated with maintaining NCIS records. Field personnel should use the corresponding operational code such as RC25 Law Enforcement Administration, CT25 CT Administration, FC25 CI Administration or AD01 General Administration.
AD10	Strategic Planning and Program Evaluation/Analysis	Management and Administration	Planning and Evaluation	N/A	Code 14 personnel to record hours spent conducting strategic planning, analysis and evaluation of NCIS programs. All NCIS employees conducting continuous process improvement/LSS projects.
AD11	Personnel	Management and Administration	Human Resources	N/A	Conducting human resources, payroll and associated functions (HQ/field).
AD12	General Management	Management and Administration	Administration	N/A	HQ and field supervisors/managers whose time cannot be recorded under more specific codes.
AD17	BRAC Planning	Management and Administration	Planning and Evaluation	N/A	Planning/implementing activities related to Base Realignment and Closure (BRAC) (All).
AD18	Suitability Investigations (2A/2S/2M)	Management and Administration	Human Resources	2A, 2S, 2M	Conducting background suitability investigations on prospective NCIS employees (HQ/field).
TR11	Training Instruction	Management and Administration	Human Resources	N/A	Providing training and executing the NCIS Training Program (All).
TR13	Training Curriculum Review, Development and Evaluation	Management and Administration	Human Resources	N/A	Preparing training course materials (Code 10B only).

TR15	Instructional, Administrative and Systems Support to Training Programs	Management and Administration	Human Resources	N/A	Technician, systems and administrative personnel supporting training (Code 10B).
TR20	Training Supervision/Management	Management and Administration	Supervision	N/A	For Code 10B to record hours expended by supervisors.
TR21	Training Liaison	Management and Administration	Human Resources	N/A	For Code 10B to record hours conducting liaison.
Cyber Codes					
Code		**Program**	**Function**	**Case Category**	**Description**
CC01	Cyber Investigations	Cyber	Cyber	5H, 5I, 5J, 5K	Cyber controlled investigations into intrusions, malicious code, and denial of service.
CC02	Cyber Operations	Cyber	Cyber	XXIP	Cyber centric operations supporting CIIP and RDA efforts. Operations supporting cyberspace requirements.
CC03	Cyber Support to Counterintelligence Investigations/Operations	Cyber	Cyber	Various	Cyber lead support to CI controlled cases.
CC04	Cyber Support to Criminal Investigations/Operations	Cyber	Cyber	Various	Cyber lead support to criminal controlled cases.
CC05	Cyber Support to Terrorism Investigations/Operations	Cyber	Cyber	Various	Cyber lead support to CT controlled cases.
CC20	Cyber Supervision/Management	Cyber	Supervision	Various	Supervision of cyber related activity.
CC25	Cyber Admin/Clerical Support	Cyber	Administration	Various	Used for all administrative support related to cyber.
Combating Terrorism Codes					
Code		**Program**	**Function**	**Case Category**	**Description**
CT01	CT Investigations	Combating Terrorism	Investigations	5T, 5Y	Any activity involving a CT investigation, to include terrorism, suspicious incidents, and special inquiry (CT investigations only).

CT02	CT Operations	Combating Terrorism	Operations	XXCO, XXEX, XXCT, XXFP (non Port Visit Support)	Any activity involving collection, exercise, CT, and FP operations, except when providing port visit support. When providing port visit support under these operations, the time should be captured under CT03 (port visit support).
CT03	Port Visit Support	Combating Terrorism	Port Visit Support	5C, 5G, XXFP (Port Visit Support)	Any activity involving port visit support, to include collection, exercise, CT, and FP operations, (b)(7)(E) briefings, liaison with law enforcement/host nation security services, and PIVAs.
CT06	JTTF Activities	Combating Terrorism	JTTF	XXJT	All activities and support to Joint Terrorism Task Forces (JTTFs).
CT07	FPD Activities	Combating Terrorism	FPD		All activities and support to Force Protection Detachments (FPDs).
CT15	DSO Deployment Support CT	Combating Terrorism	Contingency Support		Only when an employee is in a deployed or expeditionary environment. This code is for work or missions related to CT investigations or operations, regardless of the employee's discipline/function at their home office.
CT20	AT/FP/CT Supervision/Management	Combating Terrorism	Supervision		Supervision/management of any CT related activity to include efforts of program managers and ASACs that cannot be tied to a more specific operational code.
CT25	AT/FP/CT Admin/Clerical Support	Combating Terrorism	Administration		Administrative support related to any CT activity.
SE04	Protective Operations	Combating Terrorism	PSO	9A, 5V	All PSO activities (All).
SE07	STAAT Physical Security, AT and LE Training	Combating Terrorism	STAAT		All training and assistance provided by STAAT to USN/USMC operational and component commands, selected non-Navy law enforcement organizations, and foreign security services.

SE09	STAAT Assessments	Combating Terrorism	STAAT		All assessments not related to port visit support to include AIVAs, humanitarian assessments, personal security vulnerability assessments and MSC-IAs.
SE20	Security Supervision/Management	Combating Terrorism	Supervision		Supervision of any STAAT related activity.
SE25	Security Admin/Clerical Support	Combating Terrorism	Administration		STAAT administrative support personnel.
Cyber Codes					
Code		**Program**	**Function**	**Case Category**	**Description**
FC01	CI Investigations	Counterintelligence	Investigations	1s, 3s, 5s (less 5C, 5G, 5V, 5T, 5Y)	Reactive investigations concerning local security inquiries, special inquiries, espionage, contact reports, information requests, technology transfer, loss of classified material, unauthorized disclosure, leakage, and compromise.
FC02	CI Operations	Counterintelligence	Operations	XXCI, XXCE, XXCC	All CI operations excluding operations directly associated with RDA activities which should be reported under FC06.
FC03	CI Collection	Counterintelligence	Collection		The systematic acquisition of information not associated with ongoing investigations or operations concerning espionage, sabotage, terrorism, and/or other intelligence activities. This code should be used for information acquired through opportunity collection and liaison events.
FC05	CI Functional Services	Counterintelligence	Functional Services	9F, 9V, 9Z	CI functional services which enable components to conduct CI activities, including CI awareness briefings, defensive briefings, and foreign visitor briefings. CI functional services also include SCIO, CI LNO and program management functions.

FC06	RDA Activities	Counterintelligence	RTP	XXTP, XXRD, XXTA	Used to report CI support to Navy/DoD Research, Development, Test and Evaluation sites and Naval Acquisition Programs containing Critical Program Information. This includes CI functional services, investigations, collections and operations efforts in support of the above programs.
FC07	CI Activity in Support of Strategic Programs	Counterintelligence	Strategic Support		CI support to the Office of Strategic Support (OSS) mission. This code should only be used when the employee is conducting operational or investigative activity in support of the OSS mission or in response to a lead tasking from OSS. This code is for work or missions attributed or related to OSS CI investigations or operations, regardless of the employee's discipline or function at their home office.
FC08	CI Surveillance Operations	Counterintelligence	Surveillance		Supporting, preparing for or conducting CI surveillance operations.
FC09	CISO Activities	Counterintelligence	CISO		For designated Staff Counterintelligence Officers to document effort supporting their assigned command. NCIS Representatives and Counterintelligence Staff Officers are not to use this code, but are required to use SLDCADA codes that corresponded to the NCIS activities code that best describes their activity.
FC15	DSO- Deployment Support CI	Counterintelligence	Contingency Support		Only when employee is in a deployed or expeditionary environment. Used only for work or missions related to CI investigations or operations regardless of employees' discipline/function at their home office.

FC20	CI Supervision/Management	Counterintelligence	Supervision		Supervision/management of any CI related activity to include efforts of program managers and ASACs that cannot be tied to a more specific operational code.
FC25	CI Admin/Clerical Support	Counterintelligence	Administration		Administrative support related to any CI activity.
Intelligence Support Codes					
Code		**Program**	**Function**	**Case Category**	**Description**
DI01	MTAC Watch	Intelligence	Indications and Warning	N/A	DI Watch Shifts, including the Law Enforcement Desk.
DI02	DI Production	Intelligence	Production	5G	Research, analysis, and production of DI products, including responses to Requests for Information, Daily Threat Summaries, Threat Assessments, Special Analytic Reports, and annual products ISO Code 25 strategic objectives (i.e., anything chopped through Production).
DI06	Analytical Support to CT Ops and Investigations	Intelligence	Analysis	N/A	Research, analysis, and production provided ISO Code 21.
DI07	Analytical Support to CI Ops and Investigations	Intelligence	Analysis	N/A	Research, analysis, and production provided ISO Code 22.
DI09	Analytical Support to Criminal Ops and Investigations	Intelligence	Analysis	N/A	Research, analysis, and production provided ISO Code 23.
DI10	Analytical Support to Cyber Ops & Investigations	Intelligence	Analysis	N/A	Research, analysis, and production provided ISO Code 24.
DI15	Fleet Operations Group (FOG) Operations & Support	Intelligence	FOG Activities	N/A	HDI operational activity conducted by Fleet Operations Group (FOG - NCIS Code 25G) personnel.
DI18	HDI Program Management	Intelligence	HDI Program Management		(b)(7)(E)

DI19	MDA Program Management	Intelligence	MDA Program Management		Liaison and activities to fulfill director's initiatives relating to Maritime Domain Awareness (MDA), includes supervision of MDA activities.
DI20	DI Supervision/Management	Intelligence	Supervision		Supervision of DI research, analysis, and production; clerical supervision; and/or DI Program Management.
DI25	DI Admin/Clerical Support	Intelligence	Administration	-	DI administrative activities in support of analysis, research and information sharing.
Criminal Investigations Codes					
Code		**Program**	**Function**	**Case Category**	**Description**
EC01	Integrated Agent Support to Command and Fraud Surveys	Law Enforcement	Procurement Fraud	4Y	Integrated agent support or fraud surveys to an acquisition command (e.g., NAVSEA, NAVFAC).
EC02	Procurement and Major Financial Fraud	Law Enforcement	Procurement Fraud	4A, 4C, 4D, 4G, 4H, 4L, 4M, 4N, 4P, and 4X	Procurement fraud investigations such as anti-trust, defective pricing, general procurement fraud, cost mischarging, corruption, product substitution, environmental crimes, and special inquiries relating to procurement fraud.
EC03	Economic Crimes	Law Enforcement	Economic Crimes	4B, 4E, 4F, 4I, 4J, 4K, 4R, 4T, and 4U	Credit card violations, pay and allowance investigations, personnel actions, forgery (government and personal), unauthorized services and CHAMPUS violations.
EC04	FECA/Workmen's Compensation Fraud	Law Enforcement	FECA	4W	Investigations concerning workmen's compensation (i.e., Federal Employee Compensation Act (FECA)) violations.
EC05	Economic Crime and Fraud Operations	Law Enforcement	Proactive Operations	CAT 4 UO/SO	Any operation involving either general economic crimes or procurement fraud.
EC06	Fraud Awareness Briefs	Law Enforcement	Procurement Fraud	9Z	Fraud or economic crimes briefs.

EC07	Liaison (Fraud)	Law Enforcement	Procurement Fraud	N/A	Liaison conducted with other federal agencies, attorneys, or commands regarding fraud matters.
EC15	DSO-Fraud/Economic Crime Support to Deployed Military Operations	Law Enforcement	Contingency Support		Only when employee is in a deployed or expeditionary environment. Used only for work or missions related to fraud and economic criminal investigations or operations regardless of employees' discipline/function at their home office.
EC20	Procurement Fraud Supervision/Management	Law Enforcement	Supervision		Supervision/management of any economic crime or procurement fraud related activity to include efforts of program managers and ASACs that cannot be tied to a more specific operational code.
RC01	Crimes Against Persons Investigations	Law Enforcement	Reactive	7B, 7E, 7F, 7G, 7K, 7L, 7M, 7N, 7P, 7R, 7T, 7X	Reactive investigations concerning assaults, extortion, stalking, fugitives, kidnapping, missing persons, robbery, traffic accidents (w/injury), testimony offenses (e.g., perjury, false statement, etc.), and special inquiries relating to personal incidents, as well as reactive investigations involving controlled substances.
RC02	Crimes Against Property Investigations	Law Enforcement	Reactive	CAT 6s	Reactive investigations such as arson, black-marketing, identity theft, counterfeiting, postal violations, customs violations, burglary, housebreaking, larceny (government, personal, vehicle, and ordnance), wrongful destruction, bomb threats, and special inquiries relating to property incidents.
RC04	Death Investigations	Law Enforcement	Reactive	7H	Any investigation involving a death.

RC05	Family and Sexual Violence (FSV)	Law Enforcement	F&SV	7K, 7L, 7M, 7V, 8B, 8D, 8F, 8X, CAT 8 UO/SO	Reactive investigations concerning domestic violence incidents or crimes against persons with a sexual element to them, such as rape, child sex abuse, child pornography, indecent assault, sexual assault, child/adult/elder abuse, and special inquiries relating to family and sexual violence. *Special agents assigned to Family and Sexual Violence (FSV) billets who conduct child pornography or exploitation operations and resulting cases should use this code vice RC08- Proactive Criminal Operations. All other special agents conducting these types of operations will use RC08.*
RC06	Command Investigations Support (RIC)	Law Enforcement	Reactive	Various	Support given to command criminal investigators, such as Regional Investigations Coordinators (RIC), and any investigative assistance, advice, or training provided by special agents to command investigations.
RC07	Cold Case Investigations	Law Enforcement	Cold Case	7H	Any type of criminal investigation being conducted as a cold case investigation.
RC08	Proactive Criminal Operations	Law Enforcement	Crime Reduction Ops	CAT 6 and 7 UO/SO	Used for any criminal operation or investigation initiated as result of an operation, regardless of the type of operation. For example, both controlled substance and theft ring operations should be recorded under this code/ which would also include any cases initiated as a result of those operations. *The only exception are special agents assigned to FSV billets who conduct child pornography or exploitation operations, which should use RC05-Family and Sexual Violence.*

RC15	DSO- Crim Support to Deployed Military Operations	Law Enforcement	Contingency Support		Only when an employee is in a deployed or expeditionary environment. This code is for work or missions related to criminal investigations or operations, regardless of the employees' discipline/function at their home office.
RC20	Law Enforcement/Criminal Supervision/Management	Law Enforcement	Supervision		Supervision/management of any criminal investigative related activity to include efforts of program managers and ASACs that cannot be tied to a more specific operational code.
RC25	Law Enforcement/Criminal Admin/Clerical Support	Law Enforcement	Administration		Administrative support related to any criminal investigative activity including the maintenance of evidence facilities.
RC26	Crime Reduction Program	Law Enforcement	Reactive	9Z	Used to record any work, briefings, or liaison performed in furtherance of the Crime Reduction Program, regardless of campaign theme.
RC27	LE Liaison and Engagement	Law Enforcement	Reactive		(b)(7)(E)
RC97	Reserved	Law Enforcement	DSI/SI	Various	Reserved for major investigations or operations which are activated as need arises and returns to reserved status upon completion of an investigation or operation. Only NCISHQ can assign an investigation or operation to this code.
RC98	Reserved	Law Enforcement	DSI/SI	Various	Reserved for major investigations or operations which are activated as need arises and returns to reserved status upon completion of an investigation or operation. Only NCISHQ can assign an investigation or operation to this code.

RC99	Reserved	Law Enforcement	DSI/SI	Various	Reserved for major investigations or operations which are activated as need arises and returns to reserved status upon completion of an investigation or operation. Only NCISHQ can assign an investigation or operation to this code.
Miscellaneous Codes					
Code		**Program**	**Function**	**Case Category**	**Description**
BI02	Biometrics Program Management	Operations Support	Biometrics	N/A	All activities related to biometrics to include planning, program management, training and processing of fingerprints received at NCISHQ (Code 24).
CF01	Clearance Adjudication	Operations Support	Adjudication		For DONCAF adjudicative staff. Denotes time spent in the adjudication of cases and other information to include review of cases, requesting additional information, preparing correspondence, updating appropriate data bases, responding to command inquiries, and archiving information.
CF20	Central Adjudication Supervision/Management	Operations Support	Supervision		For DONCAF first and second line supervisors. Denotes all time spent in supervising teams or divisions to include personnel actions, case review, and both internal and external interface.
CF25	Central Adjudication Admin/Clerical Support	Operations Support	Administration		For DONCAF management analysts and administrative officer for all time expended. Also used by other members of Plans, Programs, and Administration Division to denote time related to administrative vice adjudicative matters.
CM01	CM Fully Instrumented (FI) Investigative Mission	Operations Support	TSCM		For use by Code 24B only.

CM03	CM Specific Phase investigative Mission	Operations Support	TSCM		For use by Code 24B only.
CM05	CM Conference Support	Operations Support	TSCM		For use by Code 24B only.
CM07	CM VIP Support	Operations Support	TSCM		For use by Code 24B only.
CM09	CM Special Operation	Operations Support	TSCM		For use by Code 24B only.
CM13	CM Travel	Operations Support	TSCM		For use by Code 24B only.
CM14	CM Liaison/ Working Group	Operations Support	TSCM		For use by Code 24B only.
CM20	CM Supervision/Management	Operations Support	Supervision		For use by Code 24B only.
FD01	Forensic Support to Criminal Investigations	Operations Support	Forensics		Forensic support to NCIS Crim/CI/CT Investigations.
FD20	Forensics Supervision/Management	Operations Support	Supervision		Forensic supervision including planning, development and evaluation.
IF01	Software/Databases	Management and Administration	Information Technology		Tier III Support for currently deployed GOTS or COTS solutions.
IF03	Network/System Administration	Management and Administration	Information Technology	N/A	Daily administration support for deployed GOTS/COTS solutions as well as Account Management.
IF04	IT Help Desk	Management and Administration	Information Technology	N/A	Non-Navy Enterprise Network (NEN) Tier 1 or Tier 2 support.
IF05	IT Watchstanding	Management and Administration	Information Technology	N/A	SPINTCOM Watchstanding Activities
IF07	Information Assurance	Management and Administration	Information Technology	N/A	Certification & Accreditation, IAVA, Network Intrusion.
IF08	IT Projects	Management and Administration	Information Technology	N/A	All IT projects less IA/CND efforts which are reported under IF07.
IF10	Information Strategy and Planning	Management and Administration	Information Technology	N/A	Development and monitoring of IT strategic planning, budget formulation and execution monitoring, business process improvement, and IT organizational communications support. IT project management/program support offices activities to be captured under IF08.

IF11	Navy Enterprise Network (NEN) Program Support	Management and Administration	Information Technology	N/A	Support for the NMCI/One-Net/IT-21/NGEN programs.
IF12	Secure Communications	Management and Administration	Information Technology	N/A	COMSEC support for secure voice, video and data.
IF13	Voice/Video Support	Management and Administration	Information Technology	N/A	Desktop and mobile voice efforts to include Blackberry support. Also includes operations and support for VTC programs
IF20	Information Systems and Support Supervision/Management	Management and Administration	Supervision	N/A	Supervision of IT resources. To be used by YC designated employees only. Project Management covered under IF08
IF25	Information Systems Support Admin/Clerical Support	Management and Administration	Administration	N/A	Administrative support to IT Operations to include procurement and asset management.
PE01	Polygraph Examination, LE, CT, CI	Operations Support	Polygraph		NCIS operational polygraph examinations (criminal, counterterrorism, counterintelligence, etc.).
PE04	Polygraph Examination-CSP/TES	Operations Support	Polygraph		NCIS CI Scope/Screening Testing Polygraphs.
PE20	Polygraph Supervision/Management/Quality Control	Operations Support	Polygraph		Supervision and quality control of polygraph examinations.
PE25	Polygraph Admin/Clerical Support	Operations Support	Polygraph		Administrative support to polygraph examinations.
PL01	Internal Personnel Inquiry	Management and Administration	Inspector General	2B, 2C	Internal personnel inquiries.
PL02	Inspection Field Visits	Management and Administration	Inspector General		Inspector General (IG) Inspections.
PL20	Inspection and Oversight Supervision/Management	Management and Administration	Supervision		Supervision of the Inspector General's office.
PL25	Inspection and Oversight Admin/Clerical Support	Management and Administration	Administration		Administrative support to the Inspector General's office.

PS01	Information and Personnel Security Programs	Operations Support	Security		Includes all facets of work related to DON information and personnel security policy management, oversight and supervision. Includes: policy development, policy implementation oversight, participation in related working groups, the DON Auto-Declassification program and other related activities.
PS02	Personnel Security Appeals Board Program	Operations Support	Security		DON PSAB operations. Includes the activities of the board members and the board president. Includes: reviewing appeals, conducting deliberations, deciding appeals, generation of correspondence, maintenance of databases, contract monitoring, report generation and other related activities.
PS20	Information and Personnel Security Supervision/Management	Operations Support	Supervision		Supervision of information and personnel security activities.
PS25	Information and Personnel Security Admin/Clerical Support	Operations Support	Administration		Administrative activity relating to information and personnel security.
TE01	Technical Services Support - CT	Operations Support	Tech Services		Technical investigative support to counterterrorism missions.
TE02	Technical Services Support - LE	Operations Support	Tech Services		Technical investigative support to law enforcement missions.
TE03	Technical Services Support - CI	Operations Support	Tech Services		Technical investigative support to counterintelligence missions.
TE20	Technical Services Supervision/Management	Operations Support	Supervision		Supervision/management of Tech missions.
TE25	Technical Services Admin/Clerical Support	Operations Support	Administration		Administrative support to Tech missions.

NCIS-1, CHAPTER 10
NCIS PERSONNEL STATUS REPORT
EFFECTIVE DATE: APRIL 2015

Table of Contents **Page**

Reference:
(a) NCIS Manual 1, Chapter 44, Manpower Management Program

10-1. Purpose. This chapter provides information and instructions on how to process personnel status updates for new recruits, internal transfers, and separations. Headquarters (HQ) activities and field offices must electronically request approval to move an employee into or out of any NCIS billet via the NCIS process commonly referred to as the Personnel Status Report (PSR). This system is accessed via Lighthouse, the NCIS web-based SharePoint environment. This chapter also establishes agency policy and procedures, along with related guidance and responsibilities, for administrative staff and managers. See Appendix A for definitions, Appendix B for the procedures and overview of the PSR, and Appendix C for a more detailed look at the PSR workflow.

10-2. Policy

a. The automated PSR serves as a link to facilitate communication between field components and HQ departments.

b. The automated PSR is NCIS's official document to request a change in an employee's status, duty location, position, and/or billet assignment. It prompts the affected activity to initiate an action that alerts Manpower (Code 14P) to determine whether the employee is being properly transferred or moved into the requested billet. It also will prompt Human Resources (Code 10) to process any required documents or related personnel information.

c. The automated PSR process is used only for employees transferring into or out of a billet. All other PSR requests involving a Standard Form 50 Personnel Action (SF-50), such as a career ladder promotion, name change, leave without pay, return to duty, time off awards, etc., will continue to follow established Code 10 policy. The automation process does not replace or supersede guidance for changing the structure or criteria for billets. (See reference (a) for guidance on billets, the semiannual adjustment cycle, and the annual agent transfer cycle.)

d. Consult the appropriate Code 10 specialist for guidance on personnel actions outside the PSR process. Failure to collaborate and seek the expertise of HQ Code 10, Code 11, Code 14, and/or Code 15 prior to an employee's status change may significantly delay pay and

entitlements (locality pay, living quarter allowance, etc.) as well as the acquisition of mission sensitive resources (NMCI phone, computer, etc.).

e. The automated PSR will enhance communications, increase visibility, and improve auditability to ensure personnel are paid appropriately and as planned and assigned to the approved agency billet structure. This will greatly decrease payroll and data errors, thereby reducing processing time. In addition, an electronic notification process will eliminate time lags associated with PSRs sitting in an inbox with no action. It will also facilitate a streamlined system for billet verification and pay code validation.

f. All relevant links and user guides are posted on the PSR page in the Planning & Manpower (14P) section, including the Archived PSR and Pending Transfer lists.

g. PSR email notifications. Lighthouse uses the NCIS Legacy email system to send notifications. NMCI users with active roles in the PSR system must ensure their Legacy email is being forwarded to their NMCI accounts. For questions about email forwarding, contact the ITSC at (b)(6) @ncis.navy.mil.

10-3. Cancellation. GEN 10A-0103, Interim PSR Guidance, Effective Date 3 May 2008; and NCIS Manual 1, Chapter 10, Personnel Status Report, dated May 2008.

10-4. Chapter sponsor. Fiscal Planning and Manpower Department, Code 14P.

APPENDIX A
DEFINITIONS

1. Billet. An authorized personnel position with specific criteria tied to a position description and mission requirements. A billet must be filled by a qualified employee with the knowledge, skills, and abilities to perform the essential functions at the level required.

2. Billet adjustment cycle. The twice-yearly cycle when billet adjustments are officially recognized and approved at the NCIS enterprise level. Enduring requirements (assignments expected to last six months or more, typically) should be requested during the planning phase of this semiannual adjustment cycle. Code 14P coordinates notification when the change cycle is to begin and end.

3. Billet identification number (BIN). A 7-digit number generated by the Navy Total Force Manpower Management System (TFMMS) when a manpower requirement, organizational header, or billet note is initially entered in TFMMS.

4. PSR. The official document that initiates the process of an employee's status change, location change, and/or billet assignment.

5. Field office support officer (FOSO). The administrative officer with responsibility for management oversight and direction of administrative and technical functions that support the operational and investigative mission of the field office and subordinate offices.

6. Program manager (PM). HQ managers with program or project responsibilities to man, train, and equip manpower resources. PMs are located in Codes 00, 10, 11, 14, 15, 22, 23, and 25.

7. Promotion. A status change while a person is continuously employed, that results in a billet or location change and higher pay grade (e.g., special agent afloat and agent transfer matters).

8. Realignment/reorganization. The permanent movement of an employee and his or her position not involving a change in position, grade, or pay (including locality pay).

9. Reassignment. A permanent status change when an employee moves from one NCIS position to another NCIS position that typically results in a salary change due to a promotion or different locality pay. Excludes temporary assignments (i.e., details) expected to last fewer than six months, such as intra-agency reassignments for emerging operational demands.

10. Resignation. A permanent separation from Federal employment initiated by the employee.

11. Retirement. A status change elected by the employee to leave Federal service. Retirement typically occurs when an employment has met or exceeded the minimum age and/or length of service requirement to receive a Federal pension and other related retirement benefits.

12. Transfer cycle. The period when Agents are moved from one duty location to another.

13. Transfer out. When an NCIS employee leaves for another Federal agency.

APPENDIX B
PSR PROCEDURES AND OVERVIEW

1. Field office support officer (FOSO) or equivalent administrative contact/office manager. The PSR is initiated from the PSR page on Lighthouse to request a personnel status change involving a change in pay (increase or decrease), a change of duty station, or a change to the employee's assigned program function and billet (includes moves within HQ and intra-field office moves). Once a draft PSR is created, automated emails will prompt management review and approval.

a. Field office approval (optional). The FOSO may coordinate and vet the action at the field office level before sending the automated PSR to the next level for approval. The draft PSR may be downloaded and converted to a file for printing.

b. Initiate PSR. The assigned administrative contact will electronically submit the draft PSR to the PM and await notification that the PSR has been validated and approved or requires correction. Any identified errors must be corrected and resubmitted to the PM so that the PSR may be finalized and completed within established Code 10 time frames. Once the PSR is final, the FOSO may access the archived report on Lighthouse.

c. PSR Schedule. The PSR request must be initiated at least two full pay periods prior to, but not more than 60 days before, the proposed effective date of the action (typically the first Sunday of the pay cycle). This ensures Code 10 has adequate time to process personnel actions and allows management sufficient time to coordinate resources (communications, security forms, etc.) for incoming or outgoing personnel. Delays may adversely impact employee pay and mission-related activities.

2. Program manager (PM). The PM will be notified by email when a draft PSR record is ready for review and approval pending Code 14P and Code 10 evaluation.

a. Approve. If the draft PSR is accurate, the PM will approve the action. The PSR then moves to the next approval.

b. Disapprove. If the draft PSR has errors, the PM must electronically return the action to the FOSO (or originator).

3. Code 14P. Code 14P is notified by email when a draft PSR record has passed initial approval by the PM. Code 14P must access the list and review for accuracy. The funding source, locality codes, and other related information must be verified to ensure the appropriate billet has been assigned and employee pay is recorded correctly.

a. Approve. If the draft PSR is accurate, Code 14P will approve the action and link billets in TWMS. The PSR then moves to the next approval level.

b. Disapprove. If the draft PSR has errors or the billet assignment is incorrect, Code 14P will electronically route the action to the originator for correction and resubmission.

4. Code 10A. Code 10A is notified by email when a PSR record has been approved by the PM

APPENDIX B (CONTINUED)
PSR PROCEDURES AND OVERVIEW

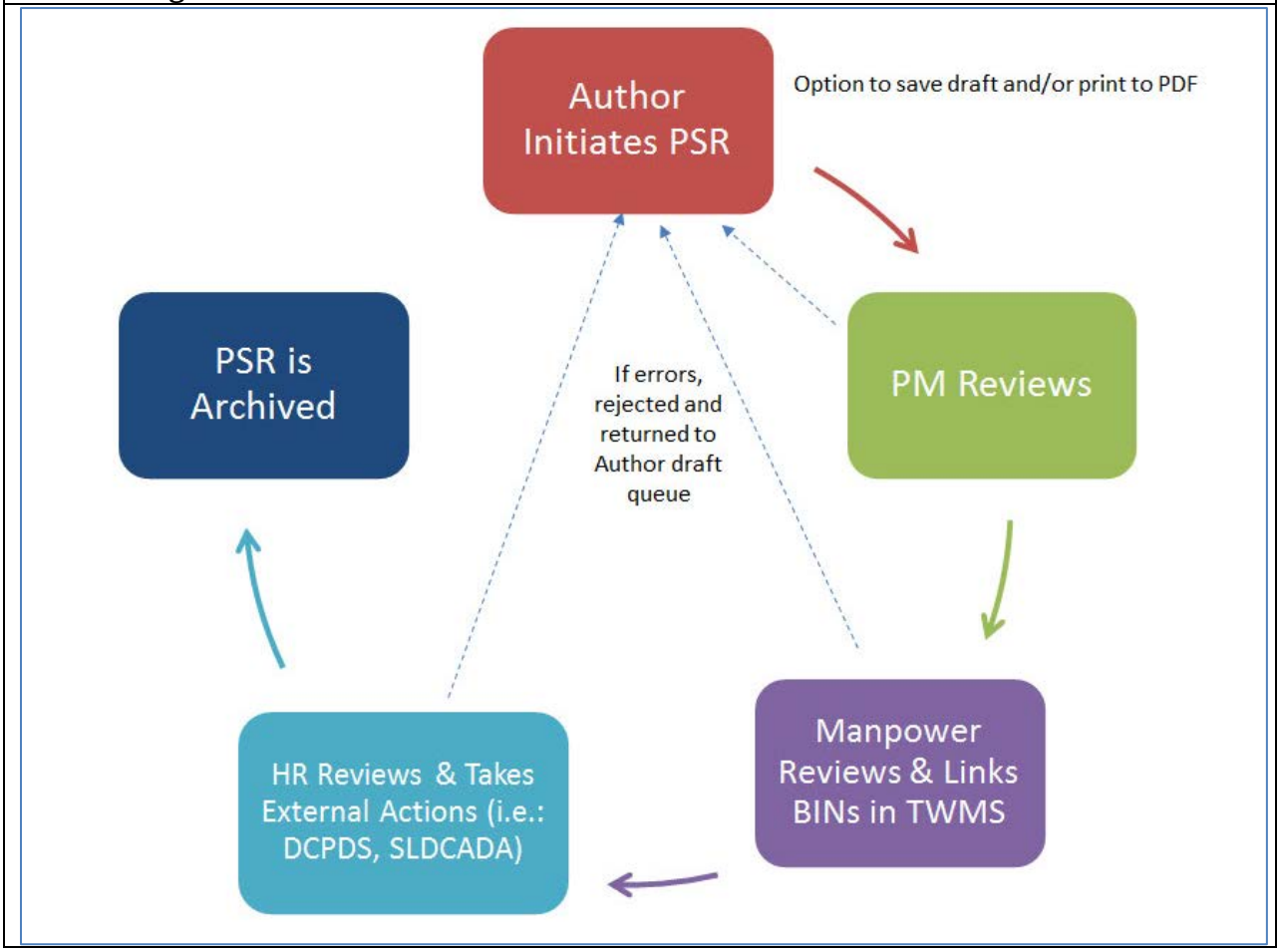
for initial approval, validated by Code 14P, and is ready for review and final validation. A determination will be made if additional personnel action is required.

a. Approve. If the draft PSR is accurate, Code 10 will approve the action and the record will be archived.

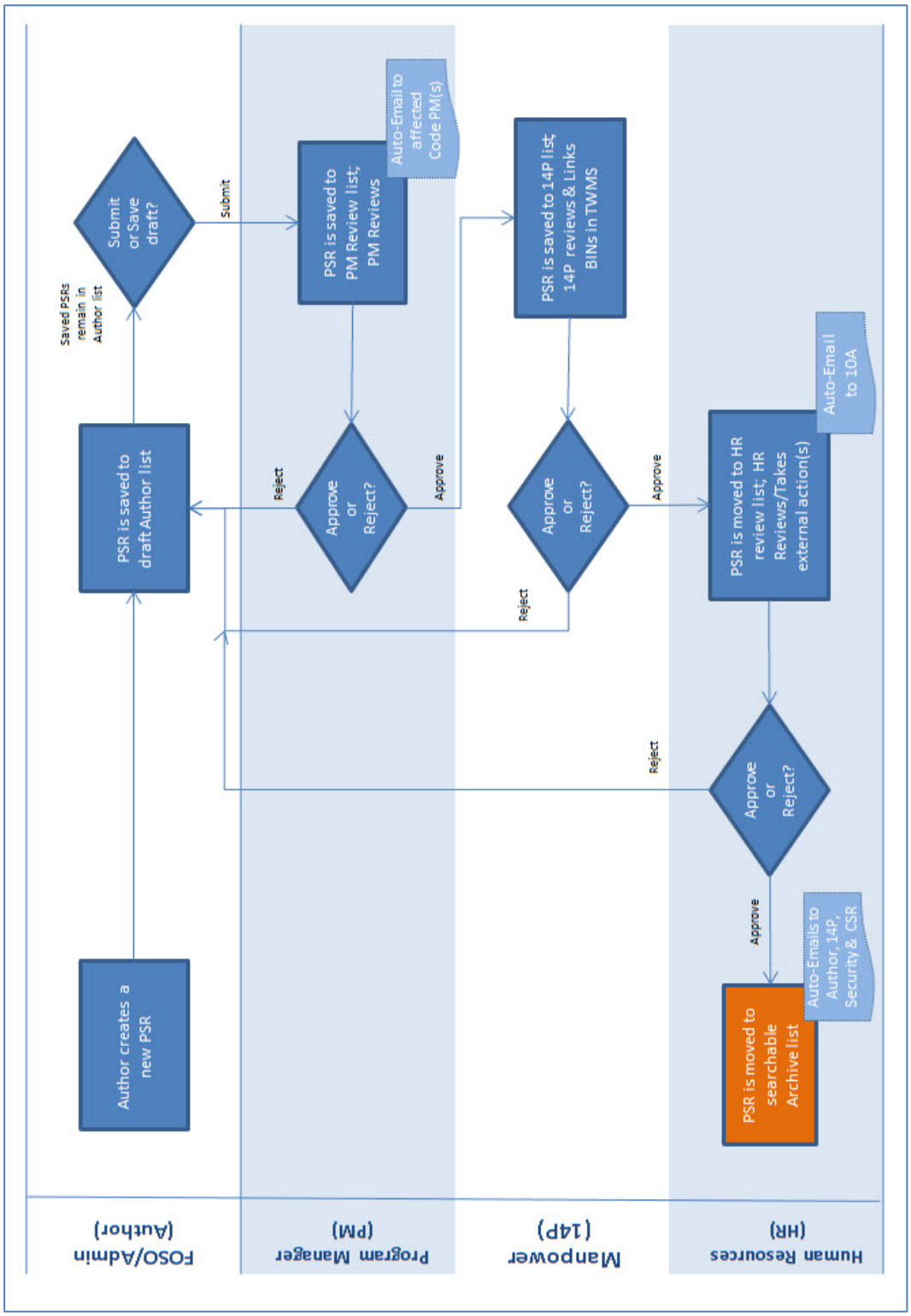
b. Disapprove. If the draft PSR has errors, Code 10 will electronically route the action to originator for correction, coordination, and resubmission.

c. Additional actions. The PSR is not final until Code 14P and Code 10 have validated and approved the request. If additional action is required, Code 10 will facilitate and ensure the appropriate personnel forms (e.g., Standard Form 52 Request for Personnel Action and SF-50) are generated.

Table 1: Lighthouse PSR Process Overview



APPENDIX C
PSR WORKFLOW DETAIL



CHAPTER 11
ESSENTIAL CIVILIAN POSITIONS
EFFECTIVE DATE: FEBRUARY 9, 2012

References:
(a) DoD Directive 1404.10, DoD Civilian Expeditionary Workforce
(b) DoD Directive 1200.7, Screening the Ready Reserve
(c) DoD Instruction 1400.25-V610 DoD Civilian Personnel Management System-Hours of Duty

11-1. Purpose. This chapter defines the policy for Emergency Essential (E-E), Non-Combat Essential (NC-E), and Mission Essential (M-E) positions and is applicable to all civilian employees who occupy those positions.

11-2. Policy

a. Naval Criminal Investigative Service (NCIS) personnel provide critical support to Department of Defense (DoD) and the Department of the Navy (DON) military forces and combat support systems in overseas positions and selected positions stateside. Paramount among the responsibilities of NCIS management is to develop and maintain appropriate resources required to ensure the rapid, efficient, and effective employment and deployment of the civilian workforce to support contingencies and emergencies. Per the guidance set forth in references (a) and (b), the Director has authority to designate such critical support billets E-E or NC-E positions and designate those in E-E/NC-E positions as key personnel. This chapter provides policy on E-E and NC-E positions, the process for designating positions E-E or NC-E, and resulting requirements for employees occupying positions designated E-E or NC-E.

b. NCIS employees perform important functions which must continue when inclement weather or other types of emergencies or situations force facilities to close to all non-essential employees. This chapter provides policy on the procedure for designating such positions M-E,

the requirements for employees who occupy M-E positions, and the necessity to establish a means of communication with all employees during closure or other emergency situations.

11-3. Cancellation. Gen Admin 11C-0006 of 25 June 2008; Subject NCIS Policy Document No. 08-01: Personnel: Emergency Essential Status.

11-4. Chapter Sponsor. The chapter sponsor is the Human Resources Directorate (Code 10). Functional management of the policies contained in this chapter is the responsibility of the Human Capital Development Department (Code 10D).

11-5. Definitions

a. Reference (a) defines E-E as "a position-based designation to support the success of combat operations or the availability of combat-essential systems." It further mandates that the DoD civilian employees who occupy those positions be designated as key in accordance with reference (b).

b. Reference (a) defines NC-E as "a position-based designation to support the expeditionary requirements in other than combat or combat support situations." It further mandates that the DoD civilian employees who occupy those positions be designated as key in accordance with reference (b).

c. Key personnel are those identified as critical to the accomplishment of the military mission and may be located overseas or in the continental United States (CONUS) and may be permanent or temporary duty assignments.

d. M-E personnel are those required to perform important functions which must continue when inclement weather or other types of emergencies or situations force facilities to close to all non-essential employees. M-E personnel will be designated by NCIS headquarters Assistant Directors (ADs) or by field office Special Agents in Charge (SACs) as described in paragraph 11-13.

11-6. Designated E-E Billets/Personnel. The following billets/personnel are designated E-E and key:

a. All special agent billets located overseas, excluding Hawaii and Alaska.

b. All intelligence specialist billets located overseas, excluding Hawaii and Alaska.

c. All deployable billets assigned to the Contingency Response Field Office.

d. All personnel comprising a Deployment Availability Roster.

e. All special agent afloat billets and deploying staff counterintelligence officer billets.

f. All special agents assigned to Protective Service billets.

11-7. Designated NC-E Billets. The following billets are designated NC-E billets and the personnel occupying them are designated as key:

a. All SAC billets located in CONUS and Hawaii.

b. All Assistant Special Agent in Charge (ASAC) billets located in CONUS and Hawaii.

c. The senior management special agent billet of any NCIS office located outside of 50 miles of the field office in CONUS or Hawaii.

11-8. Requirements for E-E/ NC-E Personnel. NCIS personnel assigned to E-E/ NC-E designated positions are required to execute a DoD Civilian Employee Overseas Emergency-Essential Position Agreement (DD Form 2365). DD Form 2365 documents that the incumbent of an E-E/NC-E position accepts certain conditions of employment arising out of crisis situations wherein he or she may be relocated either by temporary duty or permanent change of station to an overseas area or continue to work in the overseas area after the evacuation of other U.S. citizen employees who are not in E-E or NC-E positions.

11-9. E-E/NC-E Position Vacancies. For vacant E-E/NC-E designated positions, the following procedures shall be followed:

a. For E-E/NC-E positions advertised internal to NCIS, interested candidates must submit a completed DD Form 2365 to Code 10A (Professional Staff) or Code 10D (Special Agents), along with their respective resumes or bid memos. Individuals failing to submit a DD Form 2365 will not be considered for the vacancy.

b. For vacant E-E/NC-E positions advertised external to NCIS (e.g., via the Federal Government's Official Jobs Website, www.USAJOBS.gov), the selectee will be required to complete a DD Form 2365. Selectees failing to complete a DD Form 2365 will not be appointed to an E-E/NC-E position.

11-10. Newly Designated E-E/NC-E Billets. E-E/NC-E designations shall be regularly reviewed and updated as part of the NCIS operations plan. The Director has the authority to direct and assign civilian employees to E-E/NC-E positions either voluntarily or involuntarily, with or without prior notice, in order to accomplish the NCIS mission. Typically, however NCIS will attempt to provide at least 90 days notice to an employee encumbering a newly designated E-E/NC-E position. If an employee occupying a newly designated E-E/NC-E position elects not to sign the DD Form 2365, the following procedures shall be followed:

a. The employee shall continue to perform the functions of the position until a qualified replacement is available and then shall be reassigned to a vacant non-E-E/NC-E position with no loss of pay or grade.

b. If the E-E/NC-E position is overseas and the employee has not been reassigned out of the position by the end of the tour, the employee will not be extended or given a new overseas tour, unless to a non-E-E/NC-E position.

11-11. Military Reserve or National Guard. NCIS does not consider Military Reserve or National Guard status in making assignment or promotion decisions. NCIS employees who are members of the Military Reserve or National Guard should be aware of the potential impacts to their Reserve/Guard status when assigned to an E-E/NC-E position. NCIS will conduct periodic reviews to identify Military Reserve or National Guard personnel assigned to E-E/NC-E positions and report those results to respective military reserve personnel centers, per reference (b). The military reserve personnel components screen members assigned to civilian E-E/NC-E positions and determine the impact of the E-E/NC-E assignment on the military status of the member.

11-12. Administrative Dismissals and Closures Due to Inclement Weather or Other Factors

a. All NCIS civilian employees are to presume, that, unless otherwise notified, their field office or NCIS headquarters directorate, will be open each regular workday regardless of any weather or other emergency conditions which may develop. Normally, employees are expected to be prepared to cope with difficult driving conditions due to weather, interruptions of public transportation, and other situations in which significant numbers of employees are prevented from reporting to work on time or which require federal agencies to close all or part of their base/facilities.

b. Following reference (c), the commander or head of activity has the administrative authority to close all or part of an activity and to excuse administratively non-essential employees during that closure. M-E employees are expected to report for, or remain at work. Such closures are expected to be short duration, rare, and only authorized when conditions are severe or normal operations would be significantly interrupted.

c. Reference (c) further states that in geographical areas where conditions affect more than one DoD activity, the commander or head of activity employing the largest number of civilians shall make the determination whether an emergency exists and whether to administratively dismiss non-essential civilian employees. This responsibility will normally reside with a base commanding officer/commander, regional area commander or equivalent for Navy and Marine Corps bases. NCIS management will comply with the appropriate local DoD authority (or other U.S. government authority in the absence of DoD) for dismissals and base/facility closures, adapting as is prudent and provide necessary guidance for NCIS facilities located off Navy, Marine Corps, or DoD property.

11-13. Designation of M-E Positions/Employees

a. NCIS headquarters ADs and field office SACs determine what missions are "essential" under M-E conditions and what type(s) and number of personnel are needed to continue critical operations (including security and infrastructure) during group dismissals or base/facility closures resulting from severe weather conditions or other emergency situations. Because of the diversity in NCIS operations, employee occupations/skills, nature of the emergency, time of the year, geographic location, and many other factors, NCIS headquarters ADs and field office SACs are in the best position to determine their own needs based on mission requirements and/or circumstances. Factors for management to consider when designating employees as M-E include

safety and employee accessibility to the base/facility. Employees should not be needlessly exposed to hazardous conditions.

b. Telework is an effective strategy for mission accomplishment. Therefore, when considering which positions are designated M-E, NCIS headquarters ADs and field office SACs will determine if the critical operations can be accomplished via telework. If the work can be accomplished via telework, NCIS headquarters ADs and field office SACs should have the M-E employees complete a DoD Telework Agreement (DD Form 2946).

c. NCIS headquarters ADs and field office SACs will designate and inform, in writing, those M-E employees whose presence on the job is required regardless of any dismissal authorization during the workday or who must report to work regardless of any closing notice. Designations will be done annually, in September, to ensure M-E employees are fully aware of this requirement. Appendix A is a sample letter that can be used to notify employees. Supervisors shall also ensure that employees understand their responsibilities prior to an M-E situation.

d. In an extended emergency or under special circumstances, NCIS headquarters ADs and SACs may also determine that changing circumstances require non-essential employees to report for or remain at work when Government operations are disrupted and offices are closed. NCIS headquarters ADs and SACs shall establish a procedure for notifying and recalling these employees.

11-14. Communications During Emergencies/Dismissals/Closures. The ability to communicate during emergencies and other types of closure/dismissal situations is critical to ensuring the welfare of NCIS employees, as well as relaying information critical to accomplishing the mission of NCIS. Each NCIS headquarters directorate and field office shall:

a. Maintain a privacy protected recall roster with employee telephone numbers and/or email addresses so that management can communicate important information when required. The Total Workforce Management Services, MyBiz /MyWorkplace, and the Navy Family Accountability and Assessment System are tools for both collecting and retrieving employee contact data.

b. Ensure employees have a way to contact management for guidance during closure/ emergency situations.

c. Ensure all employees are familiar with closure/dismissal procedures for their local commuting area, to include the methods of determining the operating status of their facility, and policies for approving absences.

11-15. Leave Charges. M-E employees who are unable to report for, or remain at work after an official notice of dismissal or base/facility closure, must contact their chain of command immediately. In rare circumstances, a NCIS headquarters ADs or field office SACs may determine that circumstances justify excusing an M-E employee from duty. NCIS headquarters ADs or field office SACs may grant a reasonable amount of excused absence to an M-E employee who is unable to report for work when he or she has an individual hardship or

circumstances unique to the employee. For example, factors such as distance, availability of public transportation, available alternatives to childcare or eldercare, or health/medical limitations may be considered. M-E employees who do not report for or remain at work as required may be charged annual leave, sick leave, compensatory time taken, leave without pay, or absence without leave if appropriate.

Appendix A: Sample Letter for M-E Employee Designation

Date

From: (NCIS headquarters AD or field office SAC)
To: (Employee Name)

Subj: MISSION ESSENTIAL EMPLOYEE DESIGNATION

1. This letter is to inform you that you have been designated a Mission-Essential (M-E) employee for the (NCIS headquarters directorate or field office). As an M-E employee, you are required to report for, or remain at work to perform critical operations during group dismissals or base/facility closures during severe weather conditions or other emergency situations. Under certain conditions, you may be directed to perform your duties at an alternate worksite.

2. Notification of the requirement for you to report for, or remain at work will be made orally or in writing via your chain of command, or through the media, e.g, Government-wide closures. If you are unable to report for, or remain at work after an official notice of dismissal/closure, you must contact (employee name) immediately. (Employee name) will determine if your circumstance justifies excusing you from duty. Your failure to comply with a direction to report for duty as required may result in you being placed in an absent without approved leave and/or being subject to disciplinary action.

3. As a designated M-E employee, you are required to keep your contact information up to date in the Total Workforce Management Services. Please review and update your contact information by (date).

Signature of NCIS headquarters AD or field office SAC

Acknowledgement: _____
Employee's Signature Date

Copy to:
(NCIS headquarters directorate /field office)

NCIS-1, CHAPTER 12
EMPLOYEE BENEFITS
EFFECTIVE DATE: SEPTEMBER 28, 2011

Contents

References:
(a) DODI 1000.27 Mass Transportation Benefit Program
(b) Executive Order 13150, Federal Workforce Transportation
(c) 5 CFR, Chapter I, Part 831 Civil Service Retirement
(d) 5 CFR, Chapter I, Part 842 Federal Employees Retirement System
(e) 5 CFR, Chapter I, Part 870 Federal Employees Group Life Insurance Program
(f) 5 CFR, Chapter, Chapter I, Part 875 Federal Long Term Care Insurance Program
(g) 5 CFR, Chapter I, Part 890 Federal Employees Health Benefits Program
(h) 5 CFR, Chapter I, Part 894 Federal Employees Dental and Vision Insurance

12-1. Purpose. This chapter complies with references (a) through (h) and describes benefits available to employees of the Naval Criminal Investigative Service (NCIS).

12-2. Policy. It is NCIS policy to offer and administer civilian employee benefits in compliance with Office of Personnel Management, Department of Defense and Department of the Navy (DON) regulations and guidance. This chapter applies to all NCIS civilian employees.

12-3. Cancellation. This chapter replaces NCIS-1, Chapter 12 of May 2008.

12-4. Chapter Sponsor. The chapter sponsor is the Human Resources Directorate, Code 10, Human Resources Operations and Services, Code 10A.

12-5. General Benefits Information

a. Within the DON, employee benefits services are centralized under the DON Civilian Benefits Information Center (CBC). Web-based services are available at http://www.public.navy.mil/donhr/Benefits/ebis/Pages/Default.aspx. A telephone-based system is also available using an interactive voice response system. The Benefits Line can be reached by calling 888-320-2917, Monday through Friday, 0730 to 1930, Eastern Time.

b. Employee benefits include retirement, health insurance, life insurance, long term care insurance, flexible spending accounts, retirement/investment savings accounts, professional liability insurance and the Mass Transportation Benefit Program. Further information on these benefits is provided in the following paragraphs.

c. NCIS policy requires employees to review their Leave and Earning Statement (LES) each pay date to ensure that proper deductions have been withheld to avoid errors for which they could be indebted. It is especially important for employees to review the LES they receive for the first full pay period in January since it reflects any changes made during the Federal Benefits Open Season, held each year during November and December. Discrepancies should be reported to the Field Operations Support Officer (FOSO) or administrative point of contact, who will request resolution through the Remedy system.

d. A glossary of terms used throughout this chapter is available at Appendix (1).

12-6. Retirement. There are two major retirement systems for federal employees: the Civil Service Retirement System (CSRS) and the Federal Employees Retirement System (FERS). Both systems contain the special retirement provisions for law enforcement officers (LEO).

a. CSRS

(1) CSRS covers employees who first entered covered Federal service on or before December 31, 1983. CSRS is a defined benefit, contributory retirement system, which means that employees share in the expense of the annuities to which they become entitled. CSRS-covered employees contribute 7 percent or 7.5 percent (special agents) of their pay to CSRS and, while they generally pay no social security retirement, survivor and disability (OASDI) tax, they must pay the medicare tax (currently 1.45 percent of pay). The employing agency matches the employee's CSRS contributions.

(2) CSRS employees may increase their earned annuity by making tax deferred contributions up to the Internal Revenue Service maximum to a voluntary contribution account under the Thrift Savings Plan (TSP). There are no Government matching contributions for CSRS employees.

(3) Additional information on CSRS retirement benefits is available by downloading the CSRS Retirement Facts from the NCIS Human Resources (HR) website on the NCISnet (http://infoweb.ncis.navy.mil/agency/deptwebsites/personnel/documents/Benefits/csrs.pd).

b. FERS

(1) Eligible Federal employees who first entered the service on or after January 1, 1987, are covered by FERS. FERS is a retirement plan that provides benefits from three different sources: Basic Benefit Plan, Social Security, and the TSP. FERS employees contribute 0.8 percent of pay to their basic benefit plan, 6.2 percent (up to the maximum taxable wage base which changes each year) for the OASDI tax, plus a TSP contribution, if they elect to contribute to this program.

(2) Special agents covered by FERS pay an additional 0.5 percent toward their basic benefit plan for a total of 1.3% of pay, plus the full OASDI tax, plus any elected TSP contribution.

(3) For FERS employees, the TSP benefit is automatically established upon employment. Each pay period, an amount equal to 1 percent of basic pay is deposited by the agency into the TSP account. Employees may make additional contributions to the TSP account and the agency will make matching contributions up to a maximum of 5 percent of basic pay. Additional information on TSP is provided in section 12-11 of this chapter. Contributions are tax-deferred.

(4) Additional information on FERS retirement benefits is available by downloading FERS Retirement Information (available at http://infoweb.ncis.navy.mil/agency/deptwebsites/personnel/documents/benefits/fers.pdf) from the NCIS HR website.

c. CSRS Interim. Employees hired between 1 January 1984 (following termination of CSRS and 1 January 1987 (the implementation of FERS, were covered by a transitional system called CSRS Interim. Once FERS was launched, these employees were required to move to either FERS or CSRS Offset. Most were automatically covered by FERS. Employees who as of December 31, 1986, met the criteria outlined in subparagraph e below, could choose between the two retirement systems.

d. CSRS Offset

(1) This plan applies to employees who had a break in service that exceeded one year ending after 31 December 1983, and who had at least 5 years of creditable CSRS

service as of 1 January 1987. CSRS Offset employees are covered by both CSRS and Social Security. The employee is eligible for both a CSRS annuity upon retirement and in most cases Social Security retirement benefits. The employee may be adding to his or her already earned Social Security benefits (earned outside of federal service) and can continue to add to the Social Security retirement benefit if the individual continues to work in a job covered by Social Security after leaving federal service.

(2) Upon retiring from federal service before age 62, a CSRS Offset employee will have his or her CSRS annuity computed under the same rules that apply to CSRS-covered employees. When a CSRS Offset annuitant becomes age 62, the CSRS annuity will be reduced - *offset* - by the amount of the Social Security benefits earned during CSRS Offset service. Instead of receiving one check from OPM that reflects all CSRS service, the annuitant will receive another check from the Social Security Administration. If the annuitant earned less than 40 credits of Social Security and is therefore not eligible for Social Security retirement benefits, there is no offset to the CSRS annuity.

e. Special Retirement Provisions for Law Enforcement Officers (LEO). Special agents employed by NCIS are covered by the special retirement provisions for LEOs under their respective retirement system. Detailed information on LEO retirement eligibility requirements is available by downloading LEO Retirement Information from the NCIS HR website (http://infoweb/agency/deptwebsites/hr-new/HR%20Directorate.htm).

12-7. Health Insurance

a. Health insurance is provided through the Federal Employees Health Benefits (FEHB) Program. The FEHB Program provides a wide selection of health plan types and options. Eligible employees may choose from among fee for service, health maintenance organization, point-of-service products, high deductible and consumer-driven health plans.

b. Changes to FEHB enrollment can be made each year during the annual Federal Benefits Open Season, normally held during November and December. Changes may also be made as a result of a qualifying life event described in paragraph 12-15.

c. Health insurance premiums are withheld from an employee's salary on a pre-tax basis.

d. Specific information on health benefits may be found at the Office of Personnel Management (OPM) web site. This site allows employees to compare the costs, benefits, and features of different plans.

12-8. Supplemental Dental and Vision Insurance

a. The Federal Employee's Dental and Vision Insurance Program (FEDVIP) is supplemental insurance that covers a comprehensive range of dental and vision expenses.

Eligible employees pay the entire FEDVIP premium with no government contribution. Premiums are withheld from an employee's salary on a pre-tax basis.

b. Employees and retirees may enroll for FEDVIP benefits during the annual Federal Benefits Open Season. New and newly eligible employees can enroll within 60 days after they become eligible. Employees must be eligible for the FEHB Program in order to be eligible to enroll in FEDVIP; actual enrollment in FEHB is not required.

c. For enrollment to change or cancel current FEDVIP enrollment, employees must use the BENEFEDS web site at www.BENEFEDS.com or call 877-888-3337.

12-9. Life Insurance

a. Life insurance coverage is provided under the Federal Employees Group Life Insurance (FEGLI) Program. FEGLI provides group term life insurance, which does not build cash value. FEGLI consists of basic life insurance coverage and three options. In most cases, new Federal employees are automatically covered by basic life insurance and unless coverage is waived, premiums are automatically deducted from their pay. The cost of basic insurance is shared between the employee and the Government. The employee pays 2/3 of the total cost and the Government pays 1/3. There are no regularly scheduled open seasons to elect or increase coverage under FEGLI. Open seasons are held only when specifically scheduled by OPM.

b. If an employee is enrolled in basic life insurance, they may select one or more of three forms of optional insurance.

(1) Option A: $10,000 of additional coverage.

(2) Option B: Multiples of 1, 2, 3, 4, or 5 times annual pay (rounded to the next higher thousand).

(3) Option C: Coverage for a spouse and eligible dependent children. Employees may elect 1, 2, 3, 4 or 5 multiples of coverage. Each multiple is equal to $5,000 for the spouse and $2,500 for each eligible dependent child.

c. Enrollment in optional insurance is not automatic; employees must take action to elect the options. The employee pays the full cost of optional insurance.

d. The FEGLI Calculator (http://www.opm.gov/calculator/worksheet.asp) can be used to determine the face value of various combinations of FEGLI coverage; calculate premiums for the various combinations of coverage; see how choosing different Options can change the amount of life insurance and the premium withholdings; and see how the life insurance carried into retirement will change over time.

e. Designation of Beneficiary. Employees must designate a beneficiary if:

(1) They want life insurance benefits to be paid to a person, firm, organization, or other legal entity not listed in the order of precedence;

(2) They want benefits to be paid in a different order than the order of precedence;

(3) They want benefits to be paid to a trust established for the employee's minor children;

(4) Evidence of a valid marriage or dissolution of a marriage is not readily available;

(5) They want to designate a contingent beneficiary, or

(6) They want to designate a "common disaster" clause.

f. Completing a Designation of Beneficiary (SF 2823) is the preferred way to ensure benefits are distributed in accordance with employee wishes. Alternatively, your benefits will be distributed in accordance with a standard order of precedence. The SF 2823 is available on the Human Resources Service Center East (HRSC East) website. The completed form should be submitted directly to the HRSC East, ATTN: Civilian Benefits Center, NNSY, Building 17, Portsmouth, VA 23709-5000

12-10. Long Term Care Insurance

a. The Federal Long Term Care Insurance Program (FLTCIP) can help pay for costs of care when an enrollee can no longer perform everyday tasks independently due to chronic illness, injury, or the aging process. Long term care also includes the supervision an enrollee might need due to severe cognitive impairment, such as Alzheimer's disease.

b. Employees eligible for coverage under the FEHB Program are eligible to apply for coverage under the FLTCIP. Actual enrollment in FEHB is not required. Employees are eligible to apply for FLTCIP at any time. Certain medical conditions, or combinations of conditions, will prevent some people from being approved for coverage. Individuals must apply to find out if they are eligible to enroll.

c. More information about the FLTCIP and how to apply for coverage is available by contacting Long Term Care Partners at 800-582-3337, or by visiting the website at www.ltcfeds.com (http://www.ltcfeds.com).

12-11. Thrift Savings Plan (TSP)

a. The TSP is a retirement savings and investment plan for Federal employees. The TSP offers Federal employees the same type of savings and tax benefits that many private corporations offer their employees under "401(k)" plans. Employees covered by either CSRS or FERS can contribute to the TSP, however, participation rules are different for each group.

b. The TSP is a defined contribution plan. The retirement income that employees receive from their TSP account will depend on how much the employee (and the agency, if employees are covered by FERS) has contributed to the TSP account during their working years and the earnings on those contributions. The contributions are voluntary and are separate from the contributions to employees' FERS Basic Annuity or CSRS annuity accounts. Detailed information on TSP is available at the TSP website (https://www.tsp.gov/index.shtml).

c. FERS participants may elect to contribute any dollar amount or percentage (1 to 100) of basic pay, not to exceed the Internal Revenue Code limit, which is set each year by the Internal Revenue Service (IRS). FERS participants receive:

(1) Agency Automatic (1%) Contribution

(2) Agency Matching Contribution up to 5 percent

(3) Immediate vesting in Agency Matching Contributions and vesting -- generally in 3 years -- in Agency Automatic (1%) Contributions

d. CSRS participants may elect to contribute any dollar amount or percentage of basic pay, not to exceed the Internal Revenue Code limit described above. CSRS participants do not receive agency contributions.

e. For all TSP participants, the plan offers:

(1) Immediate employee contributions

(2) Before-tax savings and tax-deferred investment earnings

(3) Daily valuation of accounts

(4) Low administrative and investment expenses

(5) Transfers or rollovers of eligible distributions into the TSP

(6) A choice of investment funds

(7) Ability to make contribution allocations daily

(8) Ability to make interfund transfers

(9) Loans from your own contributions and attributable earnings while you are in Federal service

(10) Catch-up contributions for participants age 50 or older

(11) In-service withdrawals for financial hardship or after age 59½

(12) Portable benefits and a choice of withdrawal options after you separate from Federal service

(13) Ability to designate beneficiaries

(14) Protection of spouses' rights for loans and withdrawals and recognition of qualifying court orders

(15) A web site (https://www.tsp.gov/index.shtml) with general account information, capability for requesting interfund transfers and contribution allocations, the option of initiating (and in some cases completing) loan and withdrawal requests online, up-to-date TSP materials and information, online quarterly and annual participant statements, and calculators to estimate account growth, loan payments, monthly payments, and annuity amounts, as well as an elective deferral calculator. (Separated employees can also update their address information on the Web.)

(16) An automated telephone service (the ThriftLine) for account information and certain transactions

f. Changes to an employee's TSP account must be made through the TSP website (https://www.tsp.gov/index.shtml) or by calling The Thriftline at 877-968-3778 (TDD 877-847-4385).

12-12. Flexible Spending Accounts

a. Employees can elect to participate in the Federal Flexible Spending Account Program (FSAFEDS). The FSAFEDS offers three different flexible spending accounts (FSAs): a health care flexible spending account, a limited expense health care flexible spending account, and a dependent care flexible spending account.

b. Current employees can enroll in FSAFEDS each year during the Federal Benefits Open Season (November/December timeframe). Enrollments are effective January 1 of the following year. Current enrollees must remember to enroll each year to continue participating in FSAFEDS. Enrollment does NOT carry forward year to year.

c. New and newly eligible employees who wish to enroll in FSAFEDS must do so within 60 days after they become eligible, but before October 1 of the calendar year.

d. IRS regulations stipulate that any money remaining in an employee's FSA account after March 15 of the following year, for which the employee has not incurred eligible expenses, cannot be rolled over. It is important for employees to plan carefully when deciding on how much to allot in their FSA account(s). The FSAFEDS web site contains calculators to help employees determine annual allotments.

e. Detailed information on FSAFEDS can be found at www.FSAFEDS.com or by calling 877-372-3337 (TTY 800-952-0450).

12-13. Mass Transportation Benefit Program (MTBP)

a. Qualified NCIS employees are eligible to participate in the DoD Mass Transportation Benefit Program designed to offset commuting costs and expand transportation alternatives for employees. Employees may receive transit passes in the form of fare cards or vouchers in amounts equal to their personal commuting costs, not to exceed the current established limit.

b. Eligibility. This program covers NCIS employees who work in the National Capital Region (NCR), which is defined as the District of Columbia, Montgomery and Prince George's counties in Maryland, Arlington, Fairfax, Loudoun and Prince William Counties in Virginia, as well as the cities in Maryland and Virginia within the geographic area bounded by these counties. Employees can get information on program requirements and apply for the benefit on the Washington Headquarters Service (WHS) website at WHS Online (http://www.whs.mil/DFD/PSD%20Services/Applying.cfm).

c. Restrictions. Employees may not receive a transit benefit and a parking pass at the same time. As a general rule, employees with subsidized parking (i.e., parking that is free to employees and/or paid for by the government) cannot receive transit passes. Employees who receive transit passes may not be counted as part of a DoD carpool for purposes of qualifying for a parking pass. Servicing parking offices will have the authority to make exceptions to this rule. They will notify WHS of any exceptions granted.

12.14. Professional Liability Insurance

a. Authority. Public Law 104-208 requires agencies to reimburse qualified employees for up to one-half the cost incurred for professional liability insurance, up to a maximum of $150 annually. Professional Liability Insurance is defined as liability insurance that covers:

(1) Legal liability for damages due to injuries to other persons, damage to their property, or other damage or loss to such other persons (including the expenses of litigation and settlement) resulting from or arising out of tortious act, error, or omission of the covered individual (whether common law, statutory, or constitutional) while in the performance of such individual's official duties as a qualified employee; and

(2) The cost of legal representation for the covered individual in connection with any administrative or judicial proceeding (including any investigation or disciplinary proceeding) relating to any act, error, or omission of the covered individual while in the performance of such individual's official duties as a qualified employee, and other legal costs and fees relating to any such administrative or judicial proceeding.

(3) Employee Eligibility. Employees eligible to receive reimbursement for professional liability insurance include:

(a) NCIS Special Agents, and

(b) Managers and Supervisors:

1 GS managers and supervisors whose position description cover sheets reflect supervisory or managerial in Block 11.

2 DCIPS managers and supervisor whose position description cover sheets reflect a work category of supervision/management in block 3b.

b. Employee Requests for Reimbursement. Requests for reimbursement of Professional Liability Insurance must be forwarded to the HR Operations and Services Department (Code 10A) for confirmation of an employee's eligibility for reimbursement. Requests must include the following:

(1) A completed SF-1164, Claim for Reimbursement for Expenditures on Official Business, signed by the employee.

(2) An invoice from the insurance carrier which reflects the cost of the premium, the policy number, and the name of the insurance company.

(3) Proof of payment.

c. Electronic funds transfer (EFT) information for use by the paying office.

d. Processing Reimbursement Requests for Payment. Code 10A will review the employee's request for reimbursement and certify eligibility of the employee's position. When approved, Code 10A will transmit the claims to the Defense Finance and Accounting Service, Cleveland (DFAS-CL), who will settle the claim with an electronic transfer of funds to the individual's financial institution of record.

e. If it is determined that a position does not quality for reimbursement, Code 10A will provide the employee with written notification of denial, and will specify the reason for denial.

12-15. Qualifying Life Event (QLE). QLEs are common events that may occur during or after your Federal career which may impact your benefits. QLEs may provide an opportunity to increase, reduce, or cancel coverage. Detailed information on QLEs and actions required by employees are available at the OPM website at http://www.opm.gov/insure/lifeevents/index.asp.

APPENDIX (1) Definitions

Basic Annuity. An employee's basic annuity is computed based on the employee's length of service and "high-3" average pay. The "high-3" average pay is the highest average basic pay earned during any 3 consecutive years of service.

Basic Insurance. Life insurance coverage, based on an employee's annual rate of basic pay, which an employee automatically receives unless he/she waives or cancels it.

Designation of Beneficiary**.** Notice, signed by an employee, that indicates the person(s) the employee wants to receive his/her life insurance benefits. The form generally used for life insurance designations is the SF 2823 (*Designation of Beneficiary*).

Federal Employee Group Life Insurance (FEGLI). A group term life insurance program for Federal employees and retirees. The Office of Personnel Management administers the program and sets the premiums. OPM has a contract with the Metropolitan Life Insurance Company (MetLife) to provide this life insurance.

Federal Employees Health Benefits (FEHB)**.** A health benefits program that provides different types of plans: fee-for-service with a preferred provider organization; health maintenance organizations; point-of-service; high deductible health plans; and consumer-driven health plans.

Federal Employees Dental and Vision Insurance Programs (FEDVIP). This program allows dental/vision insurance to be purchased on a group basis, which means competitive premiums and no pre-existing condition limitations. There is no Government contribution to the dental/vision premiums; however, premiums are paid on a pre-tax basis.

Flexible Spending Account (FSAFEDS). A tax-favored program that allows employees to pay for eligible out-of-pocket health care and dependent care expenses with pre-tax dollars. By using pre-tax dollars to pay for eligible health care and dependent care expenses, employees receive an immediate discount on these expenses equal to the taxes they would otherwise pay on that money.

Long Term Care Insurance (FLTCIP). Insurance offered to employees, retirees, and their families, to help pay for costs of care when enrollees need help with activities they perform every day or severe cognitive impairment, such as Alzheimer's disease.

Open Season. An annual time period set by OPM in which employees may initiate or change their benefits elections. For FEHB and FEDVIP, open season is held during November and December. For FEGLI coverage, open seasons are not held annually and are rare events.

Qualified Life Event. An event that may allow individuals eligible for the FEHB Program, FEDVIP, FEGLI or FSAFEDS to enroll, or if already enrolled, to cancel or change their enrollment outside of an Open Season.

CHAPTER 13
TITLE: SPECIAL AGENT CAREER PROGRAM
POC: CODE 10A
DATE: MAR 08

POLICY DOCUMENTS:

APPENDIX (3): Gen Admin 11C-0014 of 17 May 2011 released NCIS Policy Document No. 11-0006 Administrative (Mobility Program). Policy document 11-0006 contains revised or new policy that has not been incorporated into this chapter and should be reviewed in its entirety.

APPENDIX (4): Gen Admin 11C-0017 of 31 May 2011 released NCIS Policy Document No. 11-08 Personnel (Supervisory Special Agent Selection Process (SSA-SP). Policy Document 11-08 contains revised or new policy that has not been incorporated into this chapter and should be reviewed in its entirety.

APPENDIX (5): Gen Admin 11C- 0044 of 29 Dec 2011 released NCIS Policy Document No. 11-26: Administrative (Special Agent Physical Examination Requirements). Policy Document 11-26 contains revised or new policy that has not been incorporated into this chapter and should be reviewed in its entirety.

APPENDIX (6): Gen Admin 11C-0004 of 9 Feb 2012 released NCIS Policy Document No. 12-03: Personnel (Supervisory Special Agent Selection Process (SSA-SP). Policy Document 12-03 contains revised or new policy that has not been incorporated into this chapter and should be reviewed in its entirety.

APPENDIX (7): Gen Admin 11C-0021 of 24 Oct 2012 released NCIS Policy Document No. 12-12: Administrative (Special Agent Career Program – Mobility). Policy Document 12-12 contains revised or new policy that has not been incorporated into this chapter and should be reviewed in its entirety.

13-1. INTRODUCTION

a. This chapter covers the Naval Criminal Investigative Service (NCIS) Human Resource (HR) Directorate Personnel Operations and Services (Code 10A) Special Agent (SA) Career Program to include the initial training, trial periods, career progression, promotion processes, leadership development, mobility and other program requirements unique to the career field.

b. The objective of the SA Career Program is to provide and maintain a staff of well-qualified SA personnel to accomplish the NCIS mission with maximum effectiveness. The SA Career Program provides a systematic approach to the development and advancement of professionally qualified personnel in the SA career field.

13-2. BACKGROUND

a. Scope. The SA Career Program includes all civilian employees of NCIS covered by the criminal investigator series, GS-1811. The mission of the SA is to prevent terrorism and related hostile acts against Department of the Navy (DON) forces and installations; protect against the compromise of operations, information and systems that would cause an unacceptable risk to DON personnel and strategic assets; and reduce criminal activity and mitigate its impact on Navy and Marine Corps operational readiness. NCIS SAs operate under a strong centralized and structured program to guide career development through judicious assignment practices and professional training programs on the national and local level.

b. Mobility. Selective movement of SAs provides exposure to various investigative elements. Mobility is necessary to develop SAs who are aware of the overall DON mission and are able to respond to operational requirements rapidly and effectively. Transfer of SAs to the various field offices and NCIS Headquarters (NCISHQ) for purposes of career development is not only highly desirable, it is essential to the accomplishment of the NCIS worldwide mission. Such movements provide opportunity for breadth of experience, knowledge, improved confidence, adaptability and effectively promote professional development.

c. Investigative and Technical Specialties. The SA Career Program includes four investigative specialties (General Crimes, Fraud, Combating Terrorism, and Foreign Counterintelligence) and four technical specialties (Technical Services, Cyber, Forensics and

Polygraph). Each of the specialties includes a management commitment to equal career opportunities, challenging and rewarding work, equal pay for work of equal difficulty and complexity, and the opportunity for development of management skills and abilities.

d. Other Related Publications. For a complete review of the policies affecting the hiring, development, training and assignment of SAs, other NCIS-1 Administrative Manual chapters must be read in conjunction with Chapter 13. The list of references includes, but is not limited to:

NCIS-1 Chapter 46, Special Agent Recruiting and Hiring

NCIS-1 Chapter 14, Training

NCIS-1 Chapter 15, Hours of Work, Pay and Leave

NCIS-1 Chapter 29, Special Agent Afloat Program

NCIS-1 Chapter 30, Credentials, Badges and Protective Service Pins

13-3. TRAINING/ORIENTATION OF A NEWLY HIRED SPECIAL AGENT

Typically, a new SA will be ordered to attend the Criminal Investigator Training Program (CITP) and the Special Agent Basic Training Program (SABTP) courses shortly after coming on board. Before reporting to CITP and SABTP, the agent will be assigned directly to a field office where administrative tasks will be performed, e.g., completion of required documents. The new agent will not be involved in operational functions. If the required courses are not available within the first 30 days, the assigned field office will provide a program of field training/orientation until the agent attends the basic courses. Responsibilities of a field office in the training of newly hired agents are set forth in NCIS-1 Chapter 14. All newly hired agents who have not experienced active or reserve duty with the Navy or Marine Corps must complete the Naval Orientation Correspondence Course 16138-H. The course must be successfully completed prior to the end of the trial period. Specific information regarding this course is set forth in NCIS-1 Chapter 14.

13-4. TRIAL PERIOD

a. Formerly referred to as a "probationary" period, a trial period is the first two years of an SA's employment, irrespective of the grade level at which he/she was hired. If a former SA is re-employed after having been away for a year or longer, his/her two year trial period begins with the effective date of re-appointment. If the separation from NCIS was for less than a year, prior service is creditable towards the two-year trial period.

b. Acceptable performance during this trial period will be based not only on qualitative and quantitative factors related to productivity, commensurate with training and experience, but also on demonstrable indications that the employee possesses those qualities and traits requisite for career development. The long-term qualitative character of the SA corps depends in large measure on a judicious appraisal of performance, attitude and potential during the trial period.

c. If the SA leaves NCIS during the trial period for entry into military service, time spent

on active duty or full-time reserve duty is counted toward the completion of a trial period. If the military service is not sufficient to complete the trial period, the SA is required to complete the period upon restoration to duty with NCIS.

d. At any time during the trial period that an SA's performance falls below the acceptable level, the supervisor must notify Code 10A and complete a special Performance Appraisal Review System (PARS) evaluation. In the absence of extenuating circumstances and an affirmative recommendation to retain the SA, the Deputy Assistant Director (DAD) for Code 10A will direct termination of the agent's employment.

e. The SA who leaves NCIS prior to the completion of the Field Training Agent Program (FTAP), may be required to complete the training upon reinstatement to the SA position. This determination will be made on a case by case basis with the objective of ensuring the SA will succeed in independently carrying out all required duties and functions. Additional details pertaining to the NCIS FTAP are located within the Training Department section of the HR Directorate's webpage.

13-5. PERMANENT CHANGE OF STATION AND FIRST DUTY ASSIGNMENT

a. For purposes of the SA Career Program, a Permanent Change of Station (PCS) transfer is defined as one during which the SA is required to physically relocate from one domicile to another to accept the assignment and PCS orders are issued by Code 10A effecting the reassignment. See paragraph 13-11.e. for additional details pertaining to "qualifying" PCS moves.

b. The initial assignment of the SA to a field office or headquarters code is not considered a PCS transfer. Transportation expenses incurred as a result of this assignment are not subject to reimbursement under the Joint Travel Regulations (JTR).

13-6. CAREER DEVELOPMENT

a. Initial Appointment. The entry level for SA positions is usually GL-7; however, depending on individual qualifications, some SAs may be appointed at the GL-9 level. Current Federal employees must have at least one year of qualifying experience at the next lower grade, or, grade interval, in order to qualify for appointment at the GL-7 level.

b. Promotion to GL-9. SAs hired at the GL-7 level are eligible for promotion to the GL-9 level upon completion of one year of acceptable service. Promotion actions will be implemented by respective field offices without prior approval of NCISHQ and will be effective at the beginning of the pay period following the eligibility date. Notification of the promotion action should be forwarded to Code 10A via a Personnel Status Report (PSR). Code 10A2 will confirm accurate processing of the action in the Defense Civilian Personnel Data System (DCPDS), validate the change in Compass, and add the promotion record to the personnel folder. If the promotion of a SA to the GL-9 level is not recommended, the field office will advise Code 10A, providing rationale for the decision.

c. Promotion to GL-11. Advancement of a SA to the GL-11 grade level is dependent upon completion of at least one year of acceptable service at the GL-9 level. The field office will implement this promotion without prior approval of NCISHQ. Notification of promotion should

be forwarded to Code 10A via a PSR. Code 10A2 will confirm accurate processing of the action in DCPDS, validate the change in Compass, and add the promotion record to the personnel folder. A SA is not to be promoted to GL-11 merely because he/she has completed the required length of service. It is emphasized that GL-11 agents are expected to effectively conduct complex investigations under general supervision. For this reason, only those SAs who have demonstrated appropriate professional ability and suitable performance at the GL-9 level, and who have proven potential for GL-11 duties, will be promoted. If promotion of a SA to the GL-11 level is not recommended, the field office will advise Code 10A, providing rationale for the decision.

d. Promotion to GS-12. GS-12 positions within NCIS include a variety of professionally demanding billets at both the NCISHQ and field office levels. Included among these billets are SAs assigned to Technical Investigative Specialist, Polygraph Examiner, and special staff billets. For promotion to GS-12, the SA must meet the following prerequisites:

(1) Have a total of one year in grade at the GS-11 level; and,

(2) Have received recommendations by the SAC (or, NCISHQ DAD) and approval by the DAD for Code 10A; and,

(3) Have achieved fully successful overall performance ratings for the preceding 12-month period.

e. Promotion to GS-13. A SA is eligible for promotion to the GS-13 level when the following criteria are met, and when SACs, DADs or equivalent, have recommended their advancement.

(1) Experience as a NCIS SA at the GS-12 level for the 12 months immediately preceding the proposed effective date for promotion.

(2) A total of five years creditable service as a law enforcement officer under the Special Law Enforcement Retirement provisions of Title 5, U.S.C. Section 8336 (c); or, Title 5, U.S.C. Section 8412 (d); or, the Foreign Service Retirement and Disability System as described under Public Law 105-382; or, as a credentialed military SA with NCIS; or, with a military criminal investigative organization or a combination of service thereof.

(3) Acceptable or equivalent performance ratings of record or interim appraisals, covering the 12 months immediately preceding the proposed effective date for promotion.

f. In addition to the promotion process noted above, the Director reserves the prerogative to effect promotions to the GS-13 level for demanding assignments including, but not limited to, the following:

(1) Assignment as a SA afloat for duty aboard a deployed carrier or an amphibious ready group or similar configuration, or as the staff CI officer to deploying Fleet Commanders (2^{nd} FLT, 3^{rd} FLT, 6^{th} FLT, and 7^{th} FLT), provided they meet the criteria in current Special Agent Afloat policy; or,

(2) Assignment to the Contingency Response Field Office (CRFO) with one qualifying year as a GS-12; or,

(3) Assignment to a hard-to-fill or unique position as noted in the related vacancy announcement.

13-7. TEMPORARY PROMOTIONS AND DETAILS

a. Where it is known in advance that a position will require temporary service for more than 120 days of an employee currently occupying a lower graded position, such position will be handled through temporary promotion. Competitive merit promotion procedures are required for temporary promotions exceeding 120 days; therefore, the position will be open to bidders for a designated period of time. Because temporary fill of a position may not make it feasible to expend PCS dollars, the Director, NCIS retains the prerogative to open temporary positions only to bidders in a particular geographic area.

b. All SAs currently at the grade being advertised, or, SAs at the next lower grade with one year in grade, can request consideration for the position being advertised. Temporary promotions to supervisory positions allow individuals to enhance their leadership skills while performing as a supervisor for a temporary period of time. Current GS-13 SAs within the area of consideration may bid on temporary GS-14 supervisory positions without first having been selected for GS-13 SSA or permanent advancement to GS-14.

c. In circumstances where the assignment will be for less than 120 days, an SA may be "detailed" to the position. Details do not include a change in the employee's current rate of pay; however, time spent in the detail position will be credited towards qualification for future promotions. For instance, to be eligible for promotion to a GS-15 an individual must have one year of qualifying experience at the GS-14 level. A GS-13 detailed to a GS-14 position would receive credit for the time spent in the detail position, toward the one year requirement for promotion to GS-15.

13-8. ASSIGNMENT TO DIPLOMATIC POSTS AND FORCE PROTECTION DETACHMENTS

a. Diplomatic Posts. Assignments within an overseas U.S. Embassy or Consulate are referred to as Diplomatic Posts. Individuals assigned to these positions will be expected to conduct high-level liaison duties. Agents assigned to Diplomatic Posts will report directly to the associated field office chain of command for administrative and operational oversight. Under certain circumstances, Force Protection Detachment (FPD) positions may be co-located within the Embassy or Consulate. Under these circumstances, however, the FPD duties are separate and distinct from the liaison officer duties associated with the Diplomatic Post assignment.

b. Force Protection Detachment.

(1) The Office of the Secretary of Defense (OSD) sponsored FPD program resulted from the findings of the USS COLE Commission, which noted an immediate need for DoD Counterintelligence (CI) support to in-transit forces overseas. Consequently, the FPD primary mission is to detect and warn of threats to DoD personnel (military, civilian, and dependents) and, resources in transit at overseas locations without a permanent DoD presence. The mission

further includes serving as a "force protection-force multiplier" for the American Embassy country team in support of DoD presence in those locations. This includes encouraging host nation support for threat warning and security of DoD in-transit personnel/resources as well as providing "first responder" criminal investigative support [NCIS & Air Force Office of Special Investigations (AFOSI) only], protective service, and surge capabilities in the event of a crisis/contingency.

(2) It is the responsibility of the Program Manager for the Combating Terrorism Directorate, Code 21, to administer the FPD Program within NCIS. For additional details pertaining to the NCIS FPD program, see NCIS 3, Chapter 38: Combating Terrorism Investigations and Operations/Dec06. Additionally, the following documents contain details pertaining to the FPD program and should be reviewed as supplemental documentation:

(a) Joint Standard Operating Procedures - FPD (JSOP)/19May2003

(b) MOU between Department of State (DOS) Bureau of Diplomatic Security (DS) & DoD Counterintelligence Field Activity (CIFA) re: FPD-RSO Relationship/09May2003

(c) MOU between DOS & DoD on Security of DOD Elements and Personnel in Foreign Areas/16DEC/1997

c. Eligibility And Promotion Opportunities.

(1) GS-12/13 Opportunities: Vacancies in FPDs and Diplomatic Posts where NCIS is not the lead executive agency will be announced as either GS-13 or GS-12/13 opportunities. In some FPD locations where only one FPD SA is initially assigned, it is expected that additional CI operational personnel may be required and assigned as resources permit. These FPD positions will be announced as either GS-13 or GS-12/13 opportunities. Selections will be made based upon the needs of the service.

(2) GS-14/Temp GS-14 Opportunities: IAW the temporary promotion policy contained in this chapter, the senior or sole NCIS position at an FPD or Diplomatic Post where NCIS is the lead executive agency, will be announced as a GS-14 or Temporary GS-14 opportunity, unless the Director determines that such grade is not appropriate for a particular assignment due to the organizational structure of the U. S. Embassy/Consulate, or the nature of duties required in that location.

(3) GS-14/Temp GS-14 grade designations are in recognition of required duties, high level liaison responsibilities and consequent significant impact on the NCIS mission. Generally, these billets pertain to NCIS personnel assigned as the Resident Agent-in-Charge (RAC) of DoD FPDs, where NCIS is the executive agent, and NCIS personnel assigned to NCIS Resident Units (NCISRU) located at Diplomatic Posts. For these positions, minimum eligibility will be one year of acceptable service at the GS-13 level and a willingness to attend long-term language training if not otherwise fluent in the particular language required for that AOR. Individuals at the GS-14 level, as well as those on the current GS-14 Promotion Nomination List (PNL), are also eligible for consideration. Those selected from the PNL will be promoted to permanent GS-14 upon assumption of duties. Personnel selected for these positions, but who are not on the GS-14 PNL at the time of selection, will upon completion of their tour revert back to GS-13; unless they were selected for the GS-14 PNL and permanently promoted during their assignment.

d. Vacancy Announcements.

(1) SAs assigned to Diplomatic Posts are routinely expected to interact at the highest levels of the Diplomatic mission, as well as similar levels within the host nation. In the case of FPDs, frequent and successful association with various members of U.S. country teams is essential.

(2) Positions at FPDs and Diplomatic Posts will be advertised for fill in specific geographic locations. Vacancy announcements will contain information specific to each geographic location and related tour length. In addition to eligibility requirements noted above, although desired, it is not a requirement for candidates to be Supervisory Special Agent Selection Process (SSA-SP) certified. These are all high profile positions, which require the service of experienced, professional investigators who can demonstrate the ability to exercise sound independent judgment and acumen. Candidates must have oral and written communication skills suitable for formulating and preparing well-reasoned and sound recommendations, as well as the ability to convey his/her position(s) with senior DoD and DOS officials. In some cases, specific skill sets may be required, such as language capabilities or technical skills. All factors will be considered when making selections.

13-9. SUPERVISORY SPECIAL AGENT SELECTION PROCESS

a. The Supervisory Special Agent Selection Process (SSA-SP) is open to all qualified GS-13 SAs and those GS-12 SAs who will be eligible for promotion to GS-13 by the closing date indicated in the SSA-SP announcement. Specific timeframes for the SSA-SP are located on the "NCIS Promotion and Transfer Cycle" schedule, which is posted on the Human Resources Directorate web page. Candidates must have achieved an "acceptable" performance rating of record for the most recent 12 months of service and be willing to abide by SSA-SP participation standards and requirements outlined below. Entry into the SSA-SP will be through a competitive selection process. SSA-SP opportunities will be announced as needed based upon current and projected vacancies within the supervisory ranks.

b. The SSA-SP selection process consists of two phases. Phase I has two components: an evaluation of the candidate by the SAC or DAD and a "Paper Board". Each component has a maximum score of 33 points with a total possible score of 66 points for Phase I.

(1) SAC or DAD evaluations will include input from respective field office/code management team, who will be provided with instructions suggesting the preferred means by which to conduct evaluations. In order to evaluate and score the SSA-SP candidate, SACs/DADs will review the most recent PARS results. Following review, SACs/DADs will discuss the candidate's suitability to be an SSA with members of his/her management team having direct knowledge of the candidate's performance and capabilities. SACs/DADs will not rank candidates within their field office or NCISHQ directorate. Points given by SACs/DADs will be the candidate's raw/flat score and no further calculations are required.

(2) During the "Paper Board" process, candidates' personnel records will be reviewed at NCISHQ for performance and assignment history. Panel members will look for successful leadership experience and exposure, independent duty and/or overseas assignment experience, investigative and operational competency, breadth of experience within and/or across

disciplines, and strength of performance ratings. To ensure consistency among panel members, each candidate's history will be reviewed, with individual panel member ratings being averaged for a final score. Candidates who have served a tour at NCISHQ will be given an additional 3 points (i.e., 30 + 3 = 33 maximum points).

c. Based on scores from Phase I, and considering projected numbers of SSAs needed, a percentage of candidates will be certified to participate in Phase II of the SSA-SP. At the end of Phase I, SSA-SP candidates who do not progress to Phase II will receive a letter regarding their scores in Phase I. In addition, SACs/DADs will provide feedback to SSA-SP candidates regarding their scores and individual standing within the process.

d. Phase II consists of a writing exercise and an Oral Board with a maximum possible score of 105 points.

(1) Writing exercises will take place immediately prior to the Oral Board. Candidates will be provided with a leadership problem consisting of a hypothetical issue in a workplace setting that requires decisive resolution. Candidates will then have 30 minutes to explain and justify in writing the course of action they would take to resolve the issue. Results will then be reviewed and discussed during the oral board. Writing exercises have a maximum assessed value of 5 points.

(2) Oral Boards consist of a formal interview by a panel of senior NCIS managers and a formal presentation by the candidate on an assigned topic. Assigned panels are responsible for all SSA-SP interviews during the selection process. Panel members will participate in both the personnel file review as well as the panel interview. Interviews will follow an established and validated protocol. Interview preparation and travel instructions (e.g., time frame, location, and oral presentation topics) will be provided by separate correspondence. All Oral Board interviews will be conducted at NCISHQ, and have a maximum score of 100 points.

e. Following completion of Phase II, SSA candidates will be rank ordered with appropriate weight given to the consolidated scores received during Phase I and Phase II of the process, with total cumulative points available being 171. Individuals selected for the SSA-SP will be taken from the top of the rank ordered list, commensurate with the number of candidates needed to fill prospective vacancies.

13-10. SSA-SP FOR SPECIALIZED PROGRAMS

a. The Operational Support Directorate (OSD) Specialized Programs; Polygraph Services Division (PGSD), Cyber Department (CYBER), and Technical Services Division (TSD), experience substantial demands for support to the Global War on Terrorism and the worldwide NCIS mission. In order to meet these demands, NCIS OSD Specialized Programs will continue to grow by recruiting and training agents to become Polygraph Examiners, Cyber Investigators, and Technical Service Investigators. Paramount to the success of these vital programs is a sound infrastructure based on quality leadership and technical managerial expertise. Additionally, a clear career path must be available to encourage our highly trained specialists and technical experts to remain in their specialty. To this end, the Director has approved a separate OSD Supervisory Special Agent Selection Process (OS-SSA-SP). This process will mirror, as much as possible, the SSA-SP outlined in paragraph 13-8., but will also allow NCIS to identify, select, and develop management professionals with the specialized knowledge and technical expertise

to lead the OSD into the future.

b. The OS-SSA-SP is open to all qualified GS-13 Special Agents. GS-12 SAs who meet minimum time in-grade and experience requirements for promotion to GS-13 by the closing date of the OS-SSA-SP (PGSD, CYBER, or TSD) announcement, may also compete. Additionally, all PGSD candidates must be certified DoD Polygraph Examiners while candidates for positions within CYBER and TSD must be current in training and technical standards set by the program manager and/or DoD.

c. Candidates for all disciplines must have achieved an "acceptable" performance rating of record for the previous 12 months of service, and agree to abide by OS-SSA-SP participation standards and requirements outlined below. Entry into the OS-SSA-SP will be controlled through a competitive selection process. OS-SSA-SP opportunities will be announced as needed based upon current and projected supervisory vacancies within a Specialized Program.

d. The OS-SSA-SP consists of two phases that must be completed before a candidate can be considered for a GS-13 Specialized Program supervisory position. Phase I consists of two components: an evaluation of the OS-SSA-SP candidate by the DAD responsible for the respective Specialized Program, and, a "paper board". The total possible score for Phase I is 63 points.

(1) Specialized Program DAD evaluation of OS-SSA-SP candidates has a maximum value of 33 points. DADs will carefully evaluate OS-SSA-SP candidates after receiving instructions suggesting the preferred means to conduct evaluations. In order to evaluate and score OS-SSA-SP candidates, DADs will review candidate PARS as well as solicited input from the management team regarding candidate performance and capabilities. Points assigned by DADs will become a candidate's raw/flat score with no further calculations required.

(2) The "paper board" has a maximum value of 30 points. Panels will consist of three senior NCIS managers who will be responsible for all OS-SSA-SP interviews during a specific selection process. At least one panel member will be a Senior Manager from each specific candidate's respective Specialized Program. Candidate personnel records will be reviewed for Performance and Assignment history, specifically to identify successful leadership experience and exposure, assignment experience, investigative and operational competency, breadth of experience within the respective Specialized Program and other disciplines, as well as the strength of performance ratings. To ensure consistency among panel members, each candidate's history will be reviewed and individual panel member ratings will be averaged for a final score.

e. Based on scores from Phase I, and considering the projected number of OS-SSAs needed for each program, a percentage of candidates will be referred to participate in Phase II of the OS-SSA-SP process. At the end of Phase I, OS-SSA-SP candidates who do not progress to Phase II will receive a letter regarding their Phase I results from the appropriate NCISHQ Code 24 DAD.

f. Phase II consists of two components: a writing exercise and an oral board. The total possible score for Phase II is 105 points.

(1) Writing exercises have a maximum value of 5 points and will take place prior to

the oral board. At the beginning of a writing exercise, candidates will be provided with a leadership situation consisting of a hypothetical workplace issue that requires decisive resolution. Candidates have 30 minutes to explain and justify, in writing, the course of action he/she would take to resolve the issue. The written response will then be reviewed and discussed during the oral board.

(2) Oral boards have a maximum value of 100 points. Oral boards are a formal interview by the same panel from Phase I and will include formal presentations by candidates on an assigned topic. Interviews will follow the established and validated protocol utilized in the SSA-SP and will include scenarios specific to the candidate's Specialized Program. Interview preparation and travel instructions (e.g., time frame, location, and oral presentation topics) will be provided by separate correspondence. All oral board interviews will be conducted at NCISHQ.

g. Following completion of Phase II, OS-SSA-SP candidates will be rank ordered within their Specialized Program with appropriate weight given to consolidated scores received during Phases I and II. The total cumulative points available are 168. Individuals selected for the OS-SSA-SP will be taken from the top of the rank ordered list, commensurate with the number of candidates needed to fill prospective SSA vacancies projected for each Specialized Program. At the end of Phase II, OS-SSA-SP candidates who are not selected will receive a letter regarding their performance in Phases I and II from the appropriate Code 24 DAD. OS-SSA-SP selections will be made without regard to race, color, religion, sex, national origin, age, marital status, or non-disqualifying physical or mental handicaps. All actions will be based solely on job-related criteria.

h. OS-SSAs will remain in the OS-SSA-SP as long as they receive "acceptable" performance appraisal ratings. OS-SSAs must remain in an OS-SSA billet for a period of three years before having the option to bid on a non-OS-SSA billet. An OS-SSA who desires to be removed from an OS-SSA position must submit a request, in writing, through the appropriate chain of command. With the concurrence of senior management and acceptance by the Director, the OS-SSA may be returned to a position within the Specialized Program or assigned to another SA position outside of the Specialized Program. If an OS-SSA returns to a non-SSA position, they will be required to wait for a three-year period before re-competing in the SSA-SP.

i. To complete the OS Specialized Program career ladder and infrastructure development, an OS-SSA will be eligible to compete for Senior Management, GS-14, positions within their respective Specialized Program after completing one year in an OS-SSA-SP assignment. The Senior Management selection process will follow the same format outlined in Section 13-10; however, since these positions will be limited in number, and open only to individuals in a particular Specialized Program, the following exceptions apply:

(1) Senior Management positions will be announced individually (i.e., a Promotion Nomination List will not be prepared in advance).

(2) A Promotion Nomination Board (PNB) will be convened as each senior management position becomes vacant. PNBs will be comprised of the AD, OSD (chair), three senior managers (GS-15), and one senior manager from the candidate's Specialized Program to provide technical expertise and guidance.

j. Once promoted to a Senior Management position, individuals will be required to remain in this assignment for a minimum of three years. At the end of the three-year assignment, personnel will be eligible to bid on Senior Management GS-14 positions outside of their Specialized Program.

k. A Senior Manager at the GS-14 level in a Specialized Program will be eligible to compete for GS-15 positions after meeting the one year time in grade requirement.

l. Continued participation in the OS-SSA-SP will be based on performance and an assessment of the participant's promotion potential. Candidates selected for the OS-SSA-SP are subject to accelerated mobility and must abide by the NCIS mobility policy described in Section 13-12.

13-11. PROMOTION TO GS-14/15

a. The GS-14/15 promotion process is highly competitive. SAs who meet the criteria set forth in the vacancy announcement, may request consideration for such an opportunity. Candidates interested in promotion will be evaluated on leadership/management competencies, technical skills, breadth of work experience, diversity of assignments, and demonstrated liaison/representational skills. Emphasis will be placed on the Promotion Nomination Board's (PNB) rigorous review of the candidate's personnel file, to include the previous three performance appraisals (PARS) and supervisory promotion suitability recommendations. The PNB will interview all candidates recommended for further consideration following the personnel file review.

b. PNB membership will be based on position. The Director, NCIS will determine membership of the PNB. The GS-15 PNB will be comprised of members at the SES level and will be chaired by a voting Deputy Director. The GS-14 PNB will be comprised of GS-15 senior leaders, chaired by a voting Executive Assistant Director. PNB members will participate in both the personnel file review as well as the panel interview. Scores from personnel file reviews and interviews will be combined, resulting in a composite individual score.

c. Selection to the Promotion Nomination List (PNL) brings an expectation of availability for immediate worldwide reassignment, based on the needs of the service. Candidates will ensure their availability for transfer prior to applying for promotion.

d. The GS-14 and GS-15 promotion process normally occurs annually, however, additional boards may be convened if required. The process will be conducted as follows:

(1) Annually, Code 10A will make a determination of the number of senior leadership selections necessary based on anticipated vacancies, retirements/resignations, NCISHQ validated new leadership billets, and other billet structure and/or strategic organizational shifts. The HR Assistant Director (AD) will prepare a formal recommendation to the Director to initiate the promotion process, to include the projected number of vacancies anticipated.

(2) Upon Director, NCIS approval, Code 10A will initiate the promotion process for GS-15s and GS-14s. Specific timeframes for the promotion processes are located on the "NCIS Promotion and Transfer Cycle" schedule, posted on the Human Resources Directorate web page.

(3) Code 10A will announce initiation of the process via an administrative GEN ADMIN. Interested parties will have the opportunity to apply for placement on the PNL.

(4) Applicants must notify Code 10A of their interest in promotion by sending an e-mail or memorandum via their supervisor. Within the e-mail/memorandum, candidates shall make an affirmative statement that they fully understand the mobility policy for leadership positions and are available for immediate and worldwide transfer upon selection to the PNL.

(5) Supervisors shall forward the e-mail/memorandum with a statement addressing any significant changes in the candidate's performance since the last official PARS.

(6) Supervisors and candidates have a joint responsibility to ensure Code 10A has received the last three PARS of the candidate; that the PARS contain all pertinent performance and assignment information; that they address the candidate's proficiency in each of the competencies identified below; and that the PARS contains a recommendation clearly articulating promotional and leadership suitability.

(7) Candidates will be evaluated in both parts of the process (personnel file review and oral interview) on the following:

(a) NCIS Mission Awareness/Strategic Plan: Candidate knowledge of the mission and organization of NCIS, including an understanding of how the organization fits into the entire DON and DOD. Candidate influences others to translate the mission into action.

(b) Inter-personal Skills: Candidate considers and responds appropriately to the needs, feelings and capabilities of different people in different situations; is tactful, compassionate and sensitive; and treats others with respect. Candidate exercises good judgment by making sound decisions and perceives the impact and implications of decisions.

(c) Oral/Written Communications Skills: Candidate makes clear convincing oral presentations to individuals or groups; listens effectively and clarifies information as needed; facilitates an open exchange of ideas and fosters an atmosphere of open communication. Candidate expresses facts and ideas in writing in a clear, convincing and organized manner.

(d) Liaison/Representational Skills: Candidate develops networks and builds alliances; engages in cross-functional activities; collaborates across boundaries; and finds common ground with a widening range of stakeholders. Candidate utilizes contacts to build and strengthen internal and external support bases.

(e) Strategic Thinking/Vision: Candidate formulates effective strategies consistent with the NCIS business and organizational strategies. Candidate determines objectives and sets priorities; is proactive, anticipating potential threats or opportunities; with a long-term perspective. Candidate acts as a catalyst for organizational change; builds a shared vision with others; influences others to translate vision into action.

(f) Technical Credibility: Candidate demonstrates technical proficiency and an understanding of its impact. Candidate understands and appropriately applies procedures, requirements, regulations and policies related to NCIS specialized expertise. Candidate is able to

make sound resource decisions and to address training and development needs of staff. Candidate understands the linkages between administrative competencies and mission needs.

(8) Scores will be based on the following scale and are defined as:

5 - Outstanding: Candidate's proficiency is expert in this area. Candidate applies the competency in multiple situations without guidance; can train others on this competency.

4 - Excellent: Candidate's proficiency is extensive in this area. Candidate exhibits extensive knowledge of the competency and applies the competency with little or no guidance.

3 - Satisfactory: Candidate has applied this competency in multiple situations and assignments. Candidate applies this competency with some guidance.

2 - Poor: Candidate has difficultly demonstrating this competency due to their limited knowledge and/or experience.

0- No Rating: Candidate displays no proficiency in the competency.

(9) The PNB will convene to review and score candidate's personnel files. PNB members will execute a standardized form for each candidate that provides the opportunity to score the candidate within each competency. This will result in an initial rating of the candidates. The best-qualified candidates (those with an averaged score of 3 or above based on scoring from all PNB members) will be ranked, and a percentage of those candidates, based on the needs of the service, will progress forward to the interview phase.

(10) PNB standardized interview questions will explore the candidate's readiness to assume a position of higher responsibility and authority based on the leadership competencies stated above. The PNB will also confirm the candidate's understanding of the mobility policy and their availability for immediate and worldwide transfer if selected for the PNL. The PNB interview will also be scored. The same standardized form will be used to score the candidates in the interview phase. Both scores will then be combined for a total, overall rating.

(11) PNB members will then rank the candidates by combined score and present the list of scores only to the Director, NCIS for final selection. The Director may choose to have the NCIS Inspector General review the PNL prior to final selection.

(12) Once the Director's selection is made, the PNL will be announced via an administrative Gen Admin.

(13) The PNB Chair will provide feedback for non-selected candidates via a memorandum listing the assessed competencies and areas suggested for improvement. This feedback will be provided to candidates who were not selected for the interview phase or promotion.

e. As specific leadership vacancies occur, the Director, NCIS may or may not solicit individual interest from PNL candidates for such vacancies. The Director can make selections

for leadership positions from those candidates on the PNL, or from current incumbent leaders via lateral transfer.

f. The Director, NCIS can remove a candidate from the PNL at any time for misconduct, unacceptable performance and/or failure to adhere to the NCIS mobility policy. Candidates not promoted prior to publication of a new PNL will be re-certified and placed on the next PNL should the candidate desire to remain eligible but only after Code 10A receives a statement from the candidate's supervisor indicating performance has not changed. Re-certification is only valid for a period of three years from the original PNL date. Candidates must re-compete for PNL consideration after three years. Candidates who decline a reassignment will be immediately removed from the PNL and barred from PNL consideration for a minimum of three years.

g. The selection process will be made without regard to race, color, religion, sex, national origin, age, marital status, or non-disqualifying physical or mental handicap. Selection will be based on job-related criteria and not on favoritism, personal relationships, nepotism, or patronage.

13-12. MOBILITY PROGRAM

a. NCIS serves a worldwide clientele, including the U.S. Navy, the U.S. Marine Corps, and the Combatant Commanders. It is absolutely vital that NCIS maintain a flexible workforce prepared to respond to mission requirements wherever they may occur. In keeping with this requirement, all new hires into the SA career field are required to sign a Mobility Agreement, acknowledging their understanding that one or more overseas assignments and periodic transfers within CONUS will be required throughout their career.

b. Operational requirements are the key driver of the mobility program. However, NCIS is committed to considering the personal and career impact mobility has on its employees. To the maximum extent possible, the mobility program provides employees the opportunity to plan and volunteer for transfers. This allows employees to control and plan their professional development consistent with readiness imperatives. Selected or unrequested transfers may occur in the absence of qualified volunteers.

c. A SA who leaves NCIS and is rehired at a later date receives credit for PCS moves executed prior to the break in service, provided one year was completed at the final assignment immediately prior to the break in service; otherwise, the SA will not receive credit for the PCS transfer immediately preceding the break.

d. Mobility will not be used as a way to effect discipline; however, all SAs must recognize the potential for transfer from their current duty station when misconduct or incidents of bad judgment render the SA ineffective. Such decisions are the prerogative of the Director, NCIS. Under these circumstances, a transfer may be effected as an extraordinary need of the service regardless of the SA’s time in the Area of Operational Responsibility (AOR) or mobility exemption.

e. For purposes of this policy, an AOR consists of NCISHQ and its components and the major field offices and associated sub-offices, as listed in the NCIS-2. To determine the amount of time an individual has been in their current AOR, the individual’s transfer history will be reviewed. A PCS is the official transfer of an employee from one Permanent Duty Station (PDS)

to another. For mobility purposes, short distance transfers (i.e., PCS moves within the same AOR) will generally be considered "relocation/reassignment" PCS moves and not "qualifying" PCS moves. However, a PCS move to a new PDS that is at least 50 miles from the old PDS, and which increases the employee's daily commute by at least 10 miles, will count as a qualifying PCS move for mobility purposes and will restart the individual's AOR timeframe.

f. Special Agent Afloat tours and extended TDYs in support of the global war on terrorism (i.e., to locations such as Iraq, Afghanistan, and the Horn of Africa) are viewed favorably during the selection process. While participation in these missions is not an automatic exclusion from being selected for an unrequested transfer, it is taken into account.

g. Unique assignments requiring special qualifications or experience, and unique situations requiring responsive NCIS mission support (i.e., Desert Shield/Desert Storm, GWOT, or, general war), may require expeditious transfer of SAs. Under these circumstances, the Director, NCIS may suspend or void mobility exemptions.

h. Mobility Policy for Supervisory Personnel.

(1) For purpose of definition, the SSA-SP is comprised of three groups of participants: participants who are SSA-SP validated, but have not yet served in supervisory positions; and, participants who are SSA-SP validated and currently serve as supervisors; and, currently validated SSA-SP participants who previously served in supervisory positions pursuant to SSA-SP validation.

(2) Validated SSA-SP and PNL participants may make a written request to withdraw from the SSA-SP or PNL, addressed to Code 10A, via the SAC/DAD and Executive Assistant Director (EAD). SSA-SP/PNL participants will remain in the program pending a decision on a request to withdraw, which will be decided based on the needs of the service. Anyone granted a withdrawal will be required to wait three years before reapplying for the SSA-SP/PNL or for a supervisory position. SSA-SP participants who wish to bid on SA billets must be granted a withdrawal from the SSA-SP before they will be eligible to apply for SA positions.

(3) All currently validated SSA-SP participants (paragraph 13-8 or 13-9), all candidates on a current PNL, and any NCIS supervisor under a mobility agreement, must execute lateral reassignment orders, including lateral permanent change of station orders, when directed. Failure to execute such orders will have the following effects:

(a) SSA-SP participants who have not yet served in supervisory positions pursuant to SSA-SP validation will be withdrawn from the SSA-SP and will be required to wait three years before reapplying for the SSA-SP or for a supervisory position.

(b) SSA-SP participants who currently serve in supervisory positions, or who previously served in supervisory positions pursuant to SSA-SP validation, and all GS-1811-14/15 personnel, will be referred to the NCIS HR Directorate for appropriate action.

(4) PNL personnel under mobility agreements who refuse promotion orders will be withdrawn from the PNL and will be required to wait three years before reapplying to the PNL.

(5) Managers granted an exemption from mobility may be required to temporarily assume a non-management position at the completion of a normal tour. When the employee is mobile in the future, efforts will be made to reassign the SA to a management position consistent with the needs of the service and existing management vacancies. Depending on circumstances, managers may or may not eventually return to a management billet.

i. Exemptions from the Mobility Policy.

(1) Exemptions from the mobility program or special transfer requests for managers and non-managers will be considered under exceptional circumstances. When striking the proper balance of mission needs, fairness, and personal goals, absent extraordinary circumstances, personnel should not expect to be subject to an unrequested move when one of the following conditions are present:

(a) A first-time supervisor in their first year of a CONUS assignment; or,

(b) A first-time supervisor in the first two years of an OCONUS assignment; or,

(c) Employees serving in a headquarters assignment for less than two years; or,

(d) Employees assigned to the CRFO; or,

(e) A validated humanitarian issue; or,

(f) Transfers requiring an OCONUS to OCONUS move.

(2) In addition to the six conditions listed above and absent extraordinary needs of the service, non-supervisory personnel should not expect to be subject to a selected or unrequested move:

(a) During service in their initial NCIS assignment for less than three (3) years.

(b) When within two (2) years of mandatory retirement.

(c) OCONUS tour lengths and extensions will continue to be honored in accordance with the individual's transportation agreement.

(3) In addition, the following is a list of exemption categories for which employees may qualify and elect to request:

(a) No-Move/Homeport Written Exemption: Written "No-Move" and "Homeport" letters issued to agents who volunteered for the Special Assignment Location Program (SALP) will be honored, contingent upon billet strength validations at those locations. This program was closed to new participation in 1991.

(b) Humanitarian/Hardship Exemption: See detailed information in paragraph 13-13.

(c) Pregnancy Deferment. A temporary deferment from a compulsory move may be granted if the SA is pregnant, the SA's spouse is pregnant, or the SA has a newborn child up to 1 year of age. If one of these conditions exists, the SA may request a deferment until the newborn child reaches one year of age. Upon expiration of the deferment, the SA will be expected to transfer as determined by the needs of the agency. See paragraph 13-19d for additional information pertaining to a pregnant SA.

(d) Afloat Exemption. Agents who serve a qualifying deployed afloat tour may exercise a two or three year mobility exemption at the conclusion of the tour. Refer to NCIS-1 Chapter 29, Special Agent Afloat Program, for details on the exemption duration. This exemption will commence immediately upon completion of the afloat assignment. Agents who complete a Staff Counterintelligence Officer (SCIO) assignment with a deploying numbered fleet qualify for a three year afloat exemption.

(e) Temporary Duty Tour Exemption. One-, two-, or three-year exemptions may be offered to SAs selected for extended Temporary Duty (TDY) tours (normally a six-month duration or longer). Exemptions would commence immediately upon successful conclusion of the TDY. Duration of the TDY exemption, if offered, will be noted in the vacancy announcement.

(f) 5-Year Exemption:

(1) Agents who have executed a minimum of three PCS moves, one of which was to a Critical Readiness Office (CRO), while the office was on a CRO list, earn a five-year mobility exemption. CROs are those offices with significant, recurring, or projected shortages of personnel. SAs may exercise this exemption at their discretion at CONUS locations only. To count towards the PCS requirements for a five-year mobility exemption, the PCS move must be a "qualifying" PCS move as described in paragraph 13-11e. SAs hired prior to 1993 are presumed to have satisfied the CRO requirement and qualify for this exemption if they have executed a least three qualifying PCS moves. SAs who have conducted three TDY deployments to Iraq, Afghanistan, or the Horn of Africa (in any combination), each for a period of 90 consecutive days or more, are credited towards earning a five-year mobility exemption with either, (1) having satisfied the CRO requirement, or, (2) having satisfied one PCS move. The application of the TDY tours in lieu of the CRO or PCS requirement will be made at the SAs discretion. Appendix (1) contains two possible examples of application of the TDY credit. Other combinations of assignments may also qualify for this exemption.

(2) In view of the benefits already associated with a CRFO assignment, and due to the large number of SAs assigned there, this change in policy does not apply to SAs who conduct three TDY deployments while assigned to the CRFO.

(3) Managers may not exercise the five-year exemption while in a management position. Eligible SAs who leave management may exercise the five-year exemption in accordance with the above guidance.

(4) SAs who meet eligibility and wish to exercise this exemption must notify Code 10A in writing of their intention to exercise the exemption in place. Employees who qualify for the five-year exemption and wish to exercise their exemption may submit their request for exemption in January of each year. Employees who do not submit their exemption

requests by 31 January will be subject to transfer. Requirements for timely submission of exemption requests will assist the employee in effectively planning their personal and professional goals balanced against the needs of the service to fill vacancies. Existing approved eight-year exemptions will continue to be honored. The SAs who have exercised their five-year (or, eight-year) exemption may volunteer for reassignment during the pendency of the exemption; however, unexpired time on the exemption will be forfeited if the agent is selected for transfer.

13-13. PCS PREFERENCE SHEET

a. SAs are required to submit a PCS Preference Sheet to Code 10A from 01 - 31 August each year. Code 10A will not accept forms completed outside of this timeframe. This information is critical for maintaining a fair, consistent and predictable assignment process for our workforce, while still ensuring we meet all of our mission requirements. In the event a selected or un-requested move is required, the PCS Preference Sheet gives the agent an opportunity to advise NCISHQ in advance of their transfer preferences. Failure to submit a PCS Preference Sheet by the 31st of August may result in a possible PCS transfer without consideration of an agent's preferences, as the agent's last submission (if any) will then become the preference sheet of record. Filling out a preference sheet DOES NOT constitute a transfer request. To request a transfer, an agent must submit a separate bid memo in response to a vacancy announcement. See section 13-15f(3) for additional details regarding the bid memo process.

b. PCS Preference Sheets should be completed using the four digit office codes listed in the current NCIS-2 and must rank the agent's top five PCS location preferences for each of the following areas: NCISHQ (by Code), CONUS, OCONUS, and Critical Readiness Office (CRO) locations. CROs are those offices with significant, recurring, or projected shortages of personnel. With input from the Office of Inspections and Program Directors, Code 10A will annually validate and publish the list of designated CROs.

13-14. OVERSEAS EXTENSIONS

a. To identify potential OCONUS vacancies, information on extension preferences will be solicited from overseas personnel completing their OCONUS tours during the next fiscal year. This information will be requested via overseas SACs. Prior to requesting this information, an administrative GEN ADMIN message will be released by Code 10A informing the field that the extension request cycle is about to commence and describing the specific process that will be used to compile extension data.

b. All extension requests submitted to Code 10A must be accompanied by a SAC endorsement or non-endorsement. SACs may also choose to endorse the request for an amount of time that is different than that requested by overseas personnel. Upon receipt of the extension data, Code 10A will forward the information to the Program Directors, Executive Assistant to the Director (EAD) Atlantic (EADLANT), EAD Pacific (EADPAC), and Planning &Evaluation (P&E) for review and comments. At this phase, extension requests will be evaluated from a larger workforce planning perspective. Recipients will be given three business days to respond to Code 10A with their comments on the extension requests. Non-responses will be viewed as concurrence with the extensions and/or non-extensions. A list containing endorsed and non-endorsed extension requests will then be submitted to the Deputy Directors for final approval.

Differing positions and opinions submitted by SACs and program reviewers will be resolved by the DDO.

13-15. ASSIGNMENT REQUEST OPTIONS

a. The NCIS mission demands flexibility to respond to emerging requirements. NCIS employees seek the same flexibility to balance the equally challenging family issues connected to deployments, transfers, and other career pursuits. The NCIS organizational philosophy seeks to meet the sometimes competing demands of personal and professional life through a number of work/life programs and policies designed to create more flexible, responsible work environments to support family or personal situations.

b. Employees may be able to meet their workplace flexibility requirements through one or more of the following work/life programs and policies (see NCIS-1, Chapter 15, or, the NCIS Benefits link (http://infoweb/agency/depwebsites/personnel/benefits.html for more details):

(1) Telework

(2) Part Time Employment

(3) Various Leave Options (e.g., Annual Leave, Sick Leave, Advanced Leave, Home Leave, Leave Without Pay, Voluntary Leave Transfer Program, or Family Friendly/Family Medical Leave.

c. In those cases where employees desire assignment to a specific location, whether it involves remaining in their current location or moving to a new duty location, there are two primary options available to them: 1) the transfer process, or, 2) a Humanitarian/Hardship request.

d. Each year, NCIS conducts an OCONUS and CONUS transfer process. In doing so, one of the main objectives is to provide new assignments for overseas employees whose tours are ending and for whom extensions have not been requested or approved. This process also assists program managers with aligning their billet structure to help meet mission requirements and ensure mission success. In addition to the yearly transfer cycle, there are off-cycle vacancy announcements to fill critical or specialty billets, e.g. Special Agent Afloat. (See Section 13-16 for additional details regarding the transfer process, including required documentation, review and selection factors and projected time frames.) Yearly and off-cycle transfer processes are also available to employees requesting assignments due to special circumstances, whether personal, family, or work related. Examples of special circumstances that may prompt an employee's interest in relocating to a new duty location may include, but are not limited to, the following:

(1) Assignment with Military Spouses. Section 806 of Public Law 99-145, "Department of Defense (DoD) Authorization Act of 1986," established the Military Spouse Preference Program. This program provides job placement priority for military spouses who relocate to accompany their sponsor on a PCS move to an active duty location. Formal participation in this program is limited to the competitive service and, therefore, is not available to NCIS employees who are married to military members. NCIS recognizes that NCIS employees with military spouses face the same difficult circumstances that Public Law 99-145 was designed to address. As a result, efforts will be made to assign these employees to the area

of the transferring spouse's duty station when:

(a) An opening/operational need exists in the new area; and,

(b) The performance record and qualifications of the employee support the assignment.

Employees who want to co-locate or transfer at "no cost" on their spouse's (NCIS or non-NCIS employees) orders are entitled only to the benefits associated with the spouse's orders. Duplicate benefits will not be paid if an NCIS employee elects separate travel and transportation allowances from that of their spouse (NCIS or non-NCIS employee). For additional details pertaining to travel and transportation allowances see NCIS-1, Chapter 38.

Employees who want to collocate or transfer on their military spouse's orders must ensure contact between their spouse's detailer and the Code 10A Operations Division Chief at least 6 months prior to a possible transfer date for either spouse. Failure to do so may result in unaccompanied assignments or extended separations. For additional details pertaining to travel and transportation allowances see NCIS-1, Chapter 38.

(2) Assignment with Non-Military Spouses on Mobility Agreements. A unique set of circumstances exists when one or both spouses are subject to mobility programs. This is especially a problem when the spouses are employed by different organizations. In these cases, efforts will be made to assign employees with NCIS spouses (Note: NCIS employees related or married to each other will not necessarily be assigned in the same office and will normally not be assigned as a subordinate in the other's chain of command) or spouses whose employment involves mobility requirements similar to NCIS', to the area of the transferring spouse's new assignment location when:

(a) An opening/operational need exists at the new duty location; and,

(b) The performance record and qualifications of the employee support the assignment.

Employees who want to co-locate or transfer at "no cost" on their spouse's (NCIS or non-NCIS employees) orders are entitled only to the benefits associated with the spouse's orders. Duplicate benefits will not be paid if an NCIS employee elects separate travel and transportation allowances from that of their spouse (NCIS or non-NCIS employee). For additional details pertaining to travel and transportation allowances see NCIS-1, Chapter 38.

(3) Assignments Desired Due to Special Circumstances. In addition to the spousal mobility factors, there are a number of special circumstances (personal, family, work, etc.) that may drive an individual's desire to transfer to a specific location that do not meet the Humanitarian/Hardship threshold (see subparagraph e below).

(4) For all of the above situations, reassignments will be made in concert with advertised vacancies. All assignments are based primarily on the needs of the agency and, secondarily, on the desires of the individual. Selections will be based primarily on performance record and overall qualifications for the position; however, the no-cost aspect will be considered as a secondary factor. No cost considerations are generally limited to those scenarios where a

reassignment does not require cost orders, or where a PCS is connected to a military spouse's orders or a spouse's corporate expense related to an official move. SAs should address the circumstances impacting the request, including a spouse's mobility situation or other special circumstances, in paragraph 4 of their bid memo to ensure these issues are brought to the attention of the reviewing and selecting officials.

e. Humanitarian/Hardship Requests.

(1) NCIS civilian personnel who believe they have a severe personal hardship that qualifies them for either exemption from mobility (for those subject to the NCIS mobility policy) or for a transfer to a specifically requested location, may submit a Humanitarian/Hardship (H/H) request. The process for submitting and reviewing H/H requests is detailed herein. Such requests will only be granted in cases where it is determined that a severe hardship exists. Managers granted an H/H request might be required to temporarily assume a non-management position. However, if circumstances change sufficiently to once again allow mobility, efforts will be made to reassign the individual to a management position in accordance with existing mobility policy. Mobility exemptions will be reviewed on a recurring basis consistent with the parameters set forth in the decision memorandum granting each exemption.

(2) Humanitarian/Hardship Factors: All employees are eligible to submit an H/H request. In determining whether a request should be granted, the following factors will be considered.

(a) A severe hardship exists. Examples of possible severe personal hardships are listed in paragraph 13-12.c.

(b) The problem/situation affects the applicant, his/her immediate family, and/or any bona fide dependant to the applicant. Hereinafter, immediate family members and bona fide dependents will be jointly referred to as an "immediate family member".

(c) There is no other family member or relative who is capable of providing the necessary assistance.

(d) The applicant has made every reasonable effort to alleviate the hardship through other means such as personal leave, official correspondence, power of attorney, or with the assistance of other professionals such as lawyers, counselors, clergy, doctors, psychiatrists, etc.

(e) The applicant's presence in a designated location is required for specified reasons other than for morale or financial purposes alone.

(f) If either of the following applies:

1 The applicant's transfer is required because the applicant or the immediate family member cannot receive adequate care (medical, special education, etc.) at the current location; or,

2 The applicant's non-transfer is required because the applicant or the immediate family member would not be able to receive adequate care (medical, special education, etc.) at a prospective duty location.

(3) Possible Humanitarian/Hardship Circumstances: Applicants will not be granted an H/H exemption from mobility simply because they or their immediate family member(s) have a medical condition or special education needs. To be exempt from mobility or to be transferred to a specific location, the applicant must be able to demonstrate that the requested location is the only place the individual would be able to receive the necessary treatment, special education, etc. At a minimum, the applicant must show a severe hardship justifying the need for the move or mobility exemption in respect to the desired location. The following circumstances are examples of situations that may constitute a "severe hardship" and, therefore, may justify the granting of an H/H request:

(a) Applicant or applicant's immediate family member is currently diagnosed with a chronic, serious condition or has a medically significant disease currently being diagnosed.

(b) Severe illness (physical or mental) of applicant or applicant's immediate family member resulting in the affected person's hospitalization or scheduled hospitalization for an extended period.

(c) Special medical, psychological, developmental or special educational needs of applicant or applicant's immediate family member.

(d) Death of applicant's spouse or child.

(e) Pending legal procedures (i.e., divorce proceedings and/or child custody disputes) which will require the applicant to maintain his/her current residence for the foreseeable future.

(f) Other hardships and special circumstances may qualify for H/H actions if approved by the Director, NCIS.

(4) The following circumstances would not normally justify the granting of an H/H request:

(a) For financial or business reasons (including the operation of a family business).

(b) For personal convenience.

(c) For the purpose of attending to or assisting persons not determined to be immediate family.

(d) Due to a spouse's employment circumstances.

(e) For settling of estates (instead, applicant should use leave time, other family members' assistance, lawyers, etc.).

(f) Because employee is a single parent (exception is made for unaccompanied tours).

(5) H/H Request Procedures. When an employee believes that he/she has a severe personal hardship, he/she may submit an H/H request for consideration using the following procedures:

(a) Applicants will submit a memo to their respective SAC/DAD via their direct supervisor discussing all relevant matters. Among other things, the memo should include:

1. A detailed synopsis of the H/H issue, including the name, age, and location of immediate family member(s) experiencing the hardship. This synopsis should discuss why the applicant feels his/her situation constitutes a "severe hardship".

2. A detailed description of what has been done to alleviate the H/H problem, prior to submission of the H/H request.

3. Primary and, if desired, alternate actions requested by the applicant. It is highly recommended that applicants also list alternative preferences in their request. Examples of actions that may be taken in response to an H/H request are listed below. These actions may occur individually or in conjunction with each other. Decisions on H/H requests may not always result in precisely the actions desired by the applicant. Decisions will be based on a variety of factors, the primary factor being the needs of the service; however, every attempt will be made to match career and special family needs. This list is not all-inclusive; therefore, other actions may be deemed appropriate (and may be requested) depending on the circumstances.

a. Cancellation of PCS orders.

b. Transfer to a regional location or specific office location.

c. Exemption from the mobility policy (permanent or temporary)

d. Exemption from transfer to certain specified locations only, for example, OCONUS (H/H requests granted due to unsuitability of applicant or applicant's family members in the overseas location will not necessarily preclude the transfer of the applicant and family members to a CONUS assignment).

4. A brief statement outlining how the requested action will either alleviate or resolve the H/H issue and discussing why the situation cannot be satisfactorily resolved without the requested action.

(b) In addition to the above memo, each applicant's H/H request should include documentation supporting the request. NCISHQ will not, as a matter of routine, contact physicians, attorneys, etc., to obtain records. Therefore, if the applicant wants this information reviewed as part of his/her request, then it is the applicant's responsibility to obtain and provide this information to Code 10A via their SAC/DAD. Inclusion of supporting documentation is strongly recommended to ensure clarity and provide justification for submitting the request. Requests, which are incomplete or contain insufficient information on which to base a decision, will be held in abeyance at Code 10A until the information is provided. Some examples of supporting documentation include, but are not limited to:

1. Special Education Needs. Requests pertaining to special education needs should include a letter from school officials and medical practitioners (if applicable) detailing the special care currently provided/needed.

2. If the hardship involves pending divorce action and/or custody of dependant children, a current statement indicating actual or expected court dates should accompany the request.

3. Medical Hardships. If illness is involved, a current (within two months) statement is required from the attending physician. Medical terminology within the statement should be defined to a degree sufficient to allow a layman to understand the nature of the illness. The statement must include the diagnosis and prognosis and, if hospitalization is involved, the probable length of hospitalization. When mental illness is involved, the physician and/or mental health professional's statement(s) should include pertinent background information concerning the patient's mental health, effect of treatment on the condition, and/or the possibility/probability of recurrence at a later date.

(6) SAC/DAD Comments. SAC/DAD comments must be received by Code 10A before the applicant's request will be considered. Before submission of the request, SACs/DADs will review the request to ensure it contains necessary information and supporting documentation. When forwarding the request to Code 10A, the SAC/DAD comments should contain the following information:

(a) A definitive statement (endorsed or not endorsed); and,

(b) Comments noting any new information not contained in the applicant's request which the SAC/DAD has learned by personal interview or other contact; and,

(c) A statement addressing various factors, such as: what assistance has been provided to the applicant or the applicant's family by the current duty station; information on whether the applicant has required previous special consideration/leave, etc., due to this problem or similar circumstances; applicant's disciplinary status or pending disciplinary action; applicant's current duty status and specialty; date the individual reported to his/her current duty station; the expected impact granting or not granting applicant's request will have on the office/mission; and any other relevant information which may assist NCISHQ in their evaluation and response to the applicant's request.

(7) Processing of Request. SACs/DAD should forward H/H requests along with their comments to the Code 10A Division Chief. Upon receipt of all necessary information, Code 10A will coordinate with Code 10X (for baseline alignment) and the Operational Program Directors (for billet alignment). Once complete, the billet information and the individual's packet will be routed to Code 10 management (for input regarding HR/personnel matters), the NCISHQ Staff Psychologist (for input regarding medical/psychological matters), the NCIS Inspector General, and the Deputy Director for Management and Administration (DDM&A) for review. The DDM&A will make a final decision on the request. Once a determination is made, applicants will normally be notified via official memorandum. This review, approval/denial, and notification process will also be used for reconsideration and extension requests, as explained below.

(8) Reconsideration. If the request was denied or the action granted was not that requested by the applicant, the applicant may ask for his/her request to be reconsidered by a formal memo to Code 10A Division Chief, with SAC/DAD comments and additional substantiating documentation or rationale. Reconsideration memos should reference initial requests along with declination memos received from Code 10A. Reconsideration requests need not contain documents submitted with original requests if original requests were made within the past 12 months. If more than 12 months have passed, requests for reconsideration must contain copies of original requests as an enclosure along with additional current/relevant supporting documentation.

(9) Extensions and Cancellations. Mobility exemptions will be reviewed in accordance with parameters outlined in the memorandum granting said exemption, but no later than one year from the date of approval. Exemptions will normally expire one year from the date of the approval letter. Therefore, applicants are responsible for requesting an extension of their exemption, if they believe their circumstances warrant such action. Extension requests must be submitted at least one month prior to expiration. When requesting an extension, applicants should reference their initial request along with the authorizing memos that granted their initial request and any subsequent extensions. Additionally, the memorandum should provide updated information about the applicant's circumstances, including current supporting documentation (i.e., doctor and/or school assessments, as applicable, which were completed within the past two months). When circumstances which warranted an H/H action change, and an employee is no longer eligible for the H/H exemption, applicants must notify the Code 10A Division Chief immediately of the changed circumstances.

13-16. TRANSFERS

a. Transfers are driven, to a great extent, by overseas requirements. At the conclusion of an overseas tour, the agent who does not request and receive an extension must return to a CONUS assignment in order to compete for another OCONUS assignment. An employee departing overseas may be replaced and the overseas returnee slotted into a CONUS billet, or another OCONUS assignment. Prior to backfilling overseas assignments, P&E in consultation with the relevant Operational Program(s) will analyze billets to assess their continuing validation. If positions are not revalidated, backfills will not be provided and those positions may be eliminated from the overseas billet structure. Every consideration will be given to the choices of employees returning from overseas assignments; however, it is emphasized that these individuals will be assigned where valid openings exist.

b. An Overseas Suitability Checklist must be completed for all personnel being considered for transfer to an overseas location, including Hawaii. See paragraph 13-16 for further details.

c. Specific timeframes for the transfer cycle are located on the "NCIS Promotion and Transfer Cycle" schedule, which is posted on the Human Resources Directorate web page. The announcement and selection process will occur as follows:

(1) Annually, the DAD for Code 10A will prepare transfer lists based on input from senior managers in the field and at NCISHQ. Transfer lists are based primarily on filling management and OCONUS vacancies, and placing CONUS-bound employees into billets.

(2) Transfers will be competitive and, to the maximum extent possible, voluntary. When billet vacancies occur or are projected, billets will be revalidated, advertised by Code 10A through a vacancy announcement GEN message, and filled through a competitive bidding process. SACs/DADs are responsible for ensuring that employees at off-site locations, or, TDY within their AORs, are made aware of the information contained in the vacancy announcement. Absent unanticipated vacancies or exigent circumstances, Code 10A will normally advertise vacancies at least 90 days in advance of the reporting date. Code 10A will re-advertise vacancies for which no qualified bidders are selected. If no qualified bidders are selected after the second vacancy announcement, selected transfers will occur. If it becomes necessary to transfer an employee involuntarily, the selection process will start with evaluation of assignment histories, determination of exemptions, and evaluation of suitability. A selection will then be made based primarily on performance record/qualifications and time in place. In all cases, decisions regarding selection for a vacancy will ultimately be based on needs of the service and overall efficiency of an office.

(3) Bid Submissions.

(a) In response to Code 10A vacancy announcement Gen Admins, volunteers will be required to "bid" on announced vacancies by notifying Code 10A via e-mail of their desire for reassignment to the announced vacancies. Appropriate Code 10A POCs will be listed in vacancy announcement Gen Admins. Applicants should submit their bids directly to Code 10A POCs with a courtesy copy to their immediate supervisor. Although comments are not required from the bidder's SSA and/or ASAC/Division Chief, applicants are encouraged to submit their bid through their chain of command, with a request that it be forwarded to their respective SAC/DAD for endorsement. This allows applicants' immediate supervisors the opportunity to provide comments to respective SACs/DADs for consideration. Applicants should not wait until the last day of the bid opening before submitting requests for endorsement. By doing so, they hinder their supervisor's ability to complete and forward the necessary supervisory comments to Code 10A in a timely manner. Applicants are encouraged to follow-up with their supervisors to ensure that SAC/DAD endorsements have been submitted to Code 10A prior to the bid close date. Eligible employees are encouraged to bid on more than one vacancy.

(b) As a condition of bidding, Code 10A may require volunteers to list and rank a minimum number of vacancies. Additionally, returning OCONUS bidders may be required to include at least one headquarters code on their list of assignment preferences. Unless specified otherwise in the vacancy announcement Gen Admin, individuals submitting a bid in response to a vacancy announcement should prepare a formal memorandum (hereinafter referred to as a "bid memo") detailing their request. Bidders should keep in mind the competitive nature of the vacancy for which they are applying. One goal of the bid memo should be to show why a particular candidate is best suited for the desired position(s). With this in mind, the bid memo should address a candidate's high points. If candidates want the selection committee to know something about them, they should include that information in their bid memo. Candidates should not leave it up to their supervisors to provide this level of detailed information. Additionally, bidders should not rely on information contained in NCISHQ' records or their NCISHQ personnel file. Though updated on a regular basis, these records may not highlight or contain pertinent information associated with the bidder's qualifications for a desired position.

(c) A sample Bid Memo (Appendix (2)) is provided at the end of this chapter. This sample is not all-inclusive and may be modified to meet the needs of the applicant.

Applicants are encouraged to include the following information in their bid memo. (Bullet format is preferred and applicants should try to limit their bid memo to one page):

1. Interest: List the position for which you are competing. If you are submitting a bid for more than one position, list them in order of preference.

2. NCIS Background: A "brief" synopsis of NCIS employment history (hire date/place, transfer dates/places, current location & current assignment/specialty).

3. Training and Experience: Applicants are encouraged to include relevant training and experience details in their bid, especially those highlighting their qualifications relative to the requested assignment. Some examples include: advanced training courses, deployments, independent duties, source handling, etc., and relevant pre-NCIS employment information (i.e., Credentialed Military Special Agents, former law enforcement and/or military experience, etc.).

4. Additional Comments: Applicants should use this section to list any additional factors they wish to bring to the attention of selection board members.

(4) Follow-On Assignment Bid (FAB). A FAB bid is a proposal by an employee specifying two successive transfers, for example, a transfer to Hawaii with a follow-on assignment to San Diego. Code 10A may occasionally designate a vacancy as a FAB assignment. Any qualified employee may volunteer for designated FAB vacancies. A FAB bid will consist of a bid memo listing one or more advertised, designated FAB vacancies and one or more preferred follow-on assignment(s). Bid memos should list and rank the employee's proposed follow-on assignments in order of preference. Employees may bid on successive OCONUS assignments (for example, Kuwait with follow-on assignment to Naples, Italy).

(5) Endorsements. Unless specified otherwise in the vacancy announcement GEN, all bids require endorsement or non-endorsement comments by the employee's SAC or DAD, as applicable. SAC/DAD comments should be submitted to the Code 10A POC by the bid close date. If there are any disciplinary or performance issues with the applicant, the SAC/DAD comments should discuss this and should elaborate on how these issues would or would not affect the applicant's performance at the requested assignment. A copy of the endorsement and/or non-endorsement shall be provided to the applicant upon forwarding to the Code 10A POC. All bids and SAC/DAD comments submitted in response to a Code 10A vacancy announcement will be acknowledged via e-mail. However, if an acknowledgment has not been received by the third business day following the bid close date, the applicant should contact the Code 10A POC to ensure Code 10A received the bid and the SAC/DAD comments.

(6) Supervisory Input. Using input from supervisors, Code 10A will evaluate candidates against vacancy requirements and prepare a list of transfer recommendations. Candidates' qualifications will be evaluated against a variety of criteria, e.g., language ability/aptitude, specialized work experience and training, performance and assignment history, supervisory recommendations, time in place, and staffing requirements. Selections will be based primarily on performance record and overall qualifications for the position; however, the no-cost aspect will be considered as a secondary factor. Code 10A recommendations will be submitted to the Program Directors, EADLANT, EADPAC, and the P&E Directorate for review and comments. Additionally, SACs/DADs at the respective field offices will be provided a list of the

individuals recommended for transfer to their AORs along with the associated bid memos. The recommendations forwarded to the Program Directors and SACs/DADs are not the final selections and, therefore, should be held in confidence. Program Directors and SACs/DADs are asked to refrain from forwarding these lists to individuals outside of their upper-level chain of command. Recipients will be given three business days to respond to Code 10A with their comments on the recommendations. Non-responses will be viewed as concurrence with the recommendations. The recipients' comments and Code 10A recommendations will be submitted to the Deputy Directors for review. Differing positions and opinions submitted by recipients and Code 10A will be resolved by the DDO. Following this, a list of transfer recommendations will be submitted to the Director for final approval.

(7) Once final transfer selections have been made, Code 10A will announce the selections with a selection GEN. The selection GEN will specify a transfer timeframe (i.e., 3rd/4th Qtr FY-XX). Ninety days is considered a reasonable amount of time to conduct a PCS move; however, the actual transfer dates within the specified timeframe should be coordinated between the transferring employees, their current and pending SACs/DADs. Once the transfer date is established, it is incumbent upon the losing and gaining components to submit a Personnel Status Report (PSR) to Code 10A2 in order to effect the necessary pay changes. Failure to do so will cause delays in the processing of personnel actions that directly affect the employee's pay and entitlements. When submitting the PSR, the field office should reference the selection GEN. If the individual was selected for a position entailing a temporary or permanent promotion, that information should also be noted in the PSR. A PSR is required even if the selection does not require a PCS move from one geographical location to another.

(8) Unless specified otherwise in the announcement Gen Admin, the above process for submitting bids and endorsements will also be followed with respect to announcements soliciting volunteers for TDY assignment. If the cognizant program office is not Code 10A, the appropriate POC will be specified in the vacancy announcement.

13-17. OVERSEAS SUITABILITY

During the assignment consideration phase, supervisors at or above the SAC level will interview SAs to determine their suitability for overseas assignments, including Hawaii. The interview should be documented using the Overseas Suitability Checklist and the results forwarded to Code 10A for review and retention.

13-18. OUTSIDE EMPLOYMENT

a. Outside employment by GL/GS-1811 SAs will generally be prohibited. SA positions place high demands on an individual's time and attention. Availability and response must be assured 24 hours a day. There is an expectation on behalf of the public that SAs are fully devoted to their duties. This expectation is demonstrated by the fact that SAs are eligible for Law Enforcement Availability Pay (LEAP). SAs may, on a case-by-case basis, apply for approval to engage in outside employment. The SA will forward a memorandum requesting approval via the SSA and SAC to the DAD Code 10A. The memorandum will identify the proposed position, the expected number of hours per week the employment will take, and reason(s) for wanting the outside employment (i.e., monetary, professional). The SSA and SAC will recommend either approval or disapproval. The NCISHQ legal counsel and Inspector General will be consulted and will recommend approval or disapproval to the DAD Code 10A.

b. The term outside employment means any employment other than NCIS employment, including self-employment, employment by a third party, or participation in any business venture, whether or not there is any profit to the employee. Self-employment includes any participating interest in a business, corporation, or franchised operation. Outside employment does not include the following:

(1) Ownership of stocks or bonds, or, an employee's personal management of investments of this kind.

(2) Ownership of income-producing real estate, as long as the employee does not in any manner use official time or facilities to manage such property.

(3) Efforts expended in pursuit of a charity, fund raising for youth activities, PTA, volunteer coach for youth leagues and other volunteer community activities.

(4) Participation in Military Reserve or National Guard; however, when conflicts arise between NCIS duties and Reserve/Guard duties, the employee is expected to make every effort to resolve the conflict in the favor of NCIS.

c. No employee shall engage in any outside employment which will create or appear to create a conflict of interest, reflect adversely upon the DON/NCIS, or interfere with the employee's availability for normal duties, timely recall, or the proper and effective performance of the duties of his/her position.

d. An employee who has secured approval to engage in outside employment is not authorized to use appropriated funds or items purchased or leased through expenditures of appropriated funds in furtherance of his/her outside employment. While not all inclusive, use of the following is prohibited:

(1) Government office space.

(2) Government vehicles or Government-furnished transportation.

(3) Other government employees, including courier or messenger service.

(4) Government envelopes/mailing procedures.

(5) Typewriters, word processors, computers, reproduction equipment, bulletin boards, telephone and/or paging services.

(6) Any other item or service purchased by appropriated funds.

e. In addition, an employee who has secured approval for outside employment may not:

(1) Solicit business on Department of the Navy premises at any time.

(2) Make personal solicitations to command members who are of junior rank/grade at any time or place, whether on or off duty. This is not applicable to the one time sale of

personal property or privately owned dwelling; to the off-duty employment of NCISHQ members in retail sales; or, to situations not including solicited sales.

13-19. LIMITED DUTY STATUS

a. A Deputy Director, EAD, AD, DAD or SAC must place a subordinate SA in a Limited Duty Status (LDS) when he/she believes the SA, regardless of the nature of their assigned duties, is unable to perform the full range of assigned duties. This includes, but is not limited to the SA's ability to:

(1) Apprehend a suspected or known felon with a minimum of risk to self or others.

(2) Carry and utilize authorized weapons in full compliance with all provisions of NCIS-1, Chapter 34.

(3) Exercise sound judgment to execute search warrants/authorizations.

(4) Respond correctly to situations involving spontaneous decisions to apply or withhold deadly force, etc.

(5) Possess a top-secret security clearance and access eligibility.

(6) Be declared fit for full duty by a Federal Medical Officer during required periodic SA medical examinations, or other medical examinations directed by the designated supervisor to determine fitness for duty.

b. The NCISHQ Inspector General may place an SA in a LDS if the SA becomes the subject of an Internal Personnel Inquiry (2B) and the allegations raise questions regarding the SA's judgment, integrity or competence.

c. Supervisors who place an SA in a LDS must advise the SA, in writing, of the basis for the action, and provide a copy of the notification to the DAD Code 10A.

(1) When the LDS assignment is due to medical considerations, it must be supported by a Federal Medical Officer's Fitness for Duty Certification. Supervisors shall require a fitness for duty examination whenever there is a question about an employee's continued capacity to meet the physical or medical requirements of the SA’s position. Conditions requiring this determination may include (but, not be limited to) a broken limb; hypertension (systolic rate exceeds 150 or the diastolic rate exceeds 90); peptic ulcer; organic heart disease; epilepsy; pregnancy, to the extent it limits the SA's ability to perform the duties outlined in the position description; or a requirement for prescription medication leading to a mental, physical or other impairment, which limits the SA's ability to perform the full range of duties set forth in the position description. It is the responsibility of the SA to notify the supervisor of any situation that could impact his/her ability to perform in a full duty status.

(2) The designated supervisor shall advise the SA:

(a) Of the reasons for the examination.

(b) That failure to submit to the examination shall result in the immediate placement of the SA in an administrative leave status pending resolution of the situation.

(c) Of the SA's right to submit medical information from his or her own physician or practitioner and the agency's obligation to consider such information.

(3) In all LDS cases, the designated supervisor will advise the SA in writing of the effective date of the LDS assignment and will inform the SA that his/her authority to carry a weapon has been temporarily rescinded. A concise statement of facts necessitating the LDS will be included in the letter. Information copies of the letter will be provided to each level in the individual's chain of command. The letter will evaluate the expected duration of the LDS when a reasonable prediction can be made, as in the case of minor injury. Code 10A will be advised when the SA is returned to full duty by the designated supervisor.

d. Duty Limitations. The placement of a SA in a LDS will necessarily result in a restriction of the SA's duties. Specific limitations will be determined through direct consultation between the supervisor, the employee and the Federal Medical Officer or attending physician, as appropriate. An SA in a LDS may not be involved in any operational activity where there is a reasonable expectation that enforcement duties may be required. Due to the restriction of duty and the resultant impact on the SA's ability to respond to uncontrollable situations, SAs in a LDS will not be assigned as a duty agent and will only be utilized after the normal workday when such activity does not require the SA to be armed.

e. Appeals. SAs who do not concur with their placement into a LDS may submit a detailed rationale for their non-concurrence via their chain of supervision to the DAD Code 10A, who will present the documentation to the HR AD, the deciding authority on these issues.

13-20. PHYSICAL EXAMINATIONS

a. Periodic physical examinations of all SAs will be conducted as indicated below and certification made that the SA is physically capable of performing arduous physical duties without hazard to the SA or others. Examinations should be administered by a Navy medical officer or, if unavailable, by another Federal Medical Officer.

(1) The physical will be conducted within 30 days before or after an SA's birthday, in accordance with the following schedule:

(a) At age 24, 27, 30, 33, 36, 38, 40.

(b) Every year after age forty.

(2) The Certificate of Fitness For Duty will be forwarded to Code 10A within 30 days of completion of the physical. Due to Health Information Privacy Act (HIPA) regulations, the physical and supporting documentation will be maintained by the facility conducting the examination. For new hires, the pre-employment physical will take the place of a periodic physical for the first calendar year of employment.

(3) Field Operations Support Officers (FOSOs) will ensure physical examinations are conducted on all SA personnel as required, and to ensure all SAs meet the physical

requirements covered in this subchapter. SF-600 Record of Medical Care contains the Physical Exam Matrix for Naval Criminal Investigative Service SAs.

(4) Physical requirements for incumbent civilian SAs are the same as those described for pre-employment physicals in NCIS-1, Chapter 46.

b. Fitness for Duty. A fitness for duty physical under 5 CFR 339 may be ordered in any case where a SA is unable to perform the arduous and physically demanding duties of the position. A first-level supervisor will obtain concurrence of the next supervisory level prior to advising the employee of the requirement to report for a fitness for duty physical.

(1) If a medical officer recommends a SA as physically qualified for arduous duty even though the stated physical and medical requirements are not met, the field office SAC or a designated representative will interview the examining physician to obtain a complete evaluation of the deficiency and a clear understanding of the medical reason for certifying the SA's ability to perform all the duties of his/her position.

(2) Specific attention will be paid to the requirement for SAs to operate a motor vehicle extensively and/or to use firearms. The results of the interview with the examining physician should be forwarded to Code 10A. The DAD for Personnel Operations and Services will make the decision on retention of the employee in a SA position. Those individuals who are judged physically unqualified will be processed in accordance with 5 CFR 831 Subpart L (disability retirement) or 5 CFR 339 (medical disqualification), as appropriate.

c. When SAs are transferred to a new duty station, the FOSO will ensure that the medical record is forwarded to the gaining field office.

d. Pregnant Special Agent:

(1) For the safety of a pregnant SA, and to ensure capability for full performance of duties associated with the position, NCISHQ can direct a fitness for duty physical. A Federal Medical Officer who has an understanding of physical duties required of a SA can conduct this examination.

(2) NCISHQ may also direct the interview of a pregnant SA's personal physician. Physicians should be advised of the duties of the position and be asked to make a determination regarding a pregnant SA's ability to perform those assigned duties.

(3) If either physician determines that a pregnant SA cannot fulfill certain physical duties, then the SA will not be assigned those duties. If either physician determines a pregnant SA should not fire a weapon, then the SA may not be permitted to carry a firearm during the remainder of her pregnancy.

(4) Pregnant SAs will retain SA status, grade, and pay, and will be evaluated on performance of assigned duties.

e. Physical Fitness Program. To ensure continued health, effectiveness and longevity, SAs are encouraged to maintain high standards of physical fitness. Particular emphasis is placed on those activities that improve aerobic conditioning and cardiovascular endurance.

(1) Physical fitness and employee wellness are key issues in both the public and private sectors. Employers recognize that physical fitness pays dividends in terms of reduced sick leave, reduced disability retirements, fewer accidents, increased productivity, and higher employee morale. A higher level of fitness is particularly important to law enforcement personnel, as it increases confidence and alertness; increases the capacity to withstand fatigue and stress; and, most importantly, increases the chances of survival in a deadly force encounter.

(2) SAs are considered to be in good physical condition if they possess efficient cardiovascular respiration systems (good aerobic conditioning), moderate to low levels of body fat, and adequate levels of muscular strength, flexibility, and endurance. Individuals who possess these attributes are capable of performing daily assignments without undue risk of injury or fatigue, and possess sufficient energy reserve to meet unexpected physical challenges.

(3) The NCIS physical fitness program contains four parts. Events include sit-ups, push-ups, bend and reach, and a 1.5-mile run. These events were selected because they do not rely on complex apparatuses for preparation or administration.

(4) The Special Agent Physical Fitness Classification Table, graduated for both sex and age, enables individual SAs to assess their personal performance against national norms. These standards are designed to serve as a benchmark against which to judge personal performance, and are available through Field Office Trainers.

APPENDIX (1): EXAMPLES OF APPLICATION OF THE TDY CREDIT

EXAMPLE: Using 3 qualifying TDY assignments as one PCS Move

Agent's PCS history:
Hiring Office: SWND in Jan00
Moved to: EUNA in Jan04 (non-CRO office)
Moved to: DCWA in Jan06 (CRO office)
Conducted three qualifying TDYs (as described above)

Application of TDY Credit:
SWND to EUNA = 1st PCS
EUNA to DCWA = 2nd PCS & to a CRO

3 qualifying TDYs = would be applied as the 3rd PCS move required to earn the 5-yr mobility exemption

EXAMPLE: Using 3 qualifying TDY assignments in lieu of one CRO assignment

Agent's PCS history:
Hiring Office: SWND in Jan94
Moved to: EUNA in Jan97 (non-CRO office)
Moved to: CALE in Jan00 (non-CRO office)
Moved to: FEYK in Jan06 (non-CRO office)
Conducted three qualifying TDYs (as described above)

Application of TDY Credit:
SWND to EUNA = 1st PCS
EUNA to CALE = 2nd PCS
CALE to FEYK = 3rd PCS

3 qualifying TDYs = would be applied as the CRO assignment required to earn the 5-yr mobility exemption

APPENDIX (2): BID MEMORANDUM

BID MEMORANDUM

DATE:

FROM: Your Name, Grade, Office Code

TO: Name (Bid POC listed on announcement GEN), Office Code

CC: SAC/DAD _____, Office Code
Additional supervisors (encouraged, but not required)

SUBJ: GEN NUMBER/DATE/SUBJECT TITLE

1. **Interest:**

2. **NCIS Background:**

3. **Training and Experience:**

4. **Additional Comments:**

Sincerely,

Your Name

APPENDIX (3)

From: fox@noms-a.ncis.navy.mil [mailto:fox@noms-a.ncis.navy.mil]
Sent: Tuesday, May 17, 2011 9:15
To: (b)(6) @ncis.navy.mil
Subject: 11374935IR.doc - POLICY DOCUMENT NO. 11-0006 ADMINISTRATIVE (MOBILITY PROGRAM)

62736 09:15 20110517 IN:SSDEMAIL #10782 OUT:NCISHQWWSSD #102

GENERAL ADMINISTRATION 17MAY11

FROM: 0000 GEN: 11C-0014

TO: DIST

SUBJ: POLICY DOCUMENT NO. 11-0006 ADMINISTRATIVE (MOBILITY PROGRAM)

REFERENCES
(A) NCIS-1, Chapter 13, Special Agent Career Program/Mar08
(B) NCIS-1, Chapter 29, Special Agent Afloat Programs/Mar08

1. This policy Gen Admin updates reference (a) which sets forth the mobility program for NCIS special agents (SAs). This policy document also revises reference (b) so that policy is aligned with changes made to reference (a).

2. Revisions to the NCIS SA mobility program eliminates the five year mobility exemption, eliminates the temporary duty tour exemption, limits Contingency Response Field Office (CRFO) mobility exemptions to the initial 36-month tour and shortens the Special Agent Afloat mobility exemption from three years to 12 months. The revisions also modify policy relating to involuntary transfers.

3. The NCIS mobility program is predicated on the requirement to meet mission requirements and ensure career development, and thus it serves as a key enabler for our organization's continued success.

4. Reference (a) is modified as follows:

a. Section 13-12.c is deleted.

b. Section 13-12.i.(1)(a) is changed to read as follows: "A first-time supervisor in their first 12 months of a CONUS assignment; or,"

c. Section 13-12.i.(1)(b) is changed to read as follows: "A first-time supervisor in the first 24 months of an OCONUS assignment; or,"

d. Section 13-12.i.(1)(c) is changed to read as follows: "Employees serving in a headquarters assignment for less than 24 months; or,"

e. Section 13-12.i.(1)(d) is changed to read as follows: "Employees first 36 months assigned to the CRFO, to include Virtual CRFO; or,"

f. Section 13-12.i.(2)(a) is changed to read as follows: "During the first 36 months of service in their initial NCIS assignment,"

g. Section 13-12.i.(2)(b) is changed to read as follows: "When within 24 months of mandatory retirement."

h. Section 13-12.i.(3)(d) is changed to read as follows: "Afloat Exemption. SAs who serve a qualifying deployed special agent afloat (SAA) tour of at least 150 days (excluding pre-deployment workups) may request a 12-month mobility exemption as early as 60 days from the end of the deployment. Additionally, SAAs can submit their request anytime within the 12 months following the end of the deployment. Regardless of when the request is approved, the effective starting date of this 12 month mobility exemption is the date the afloat assignment ends as documented in a Personnel Status Report (Loss). The exemption automatically expires 12 months from this date. The SAA mobility exemption, and associated requirements, also applies to SAs who complete a Staff Counterintelligence Officer (SCIO) assignment with a deploying numbered fleet. Requests for the 12 month mobility exemption are to be submitted to Code 10D via the geographical field office which had operational control of the SAA while deployed. The NCIS-1 Chapter 29, SAA Program has further information regarding the SAA program."

i. Section 13-12.i.(3)(e) is deleted.

j. Section 13-12.i.(3)(f) is changed to read as follows: "Eight and five year exemptions: Current, formal eight year and five year mobility exemption letters previously issued to special agents who met the requirements under the old policy will be honored, contingent upon billet strength validations at those locations. The eight year mobility exemption was closed in 2008 and replaced with the five year mobility exemption program, which was subsequently closed to new participation in February 2011."

k. Section 13-16.c.(2) is changed to read as follows: "Transfers will be competitive and will be made in accordance with organizational needs. When billet vacancies occur or are projected, billets will be revalidated, advertised by Code 10D through a vacancy announcement GEN message, and filled through a competitive bidding process. SACs/DADs are responsible for ensuring that employees at off-site locations, or, TDY within their AORs, are made aware of the information contained in the vacancy announcement. Absent unanticipated vacancies or exigent circumstances, Code 10D will normally advertise vacancies at least 90 days in advance of the reporting date. If it becomes necessary to transfer an employee involuntarily, the selection process will start with evaluation of assignment histories, determination of exemptions, and evaluation of suitability. A selection will then be made based primarily on performance record/qualifications and time in place. In all cases, decisions regarding selection for a vacancy will ultimately be based on needs of the service and overall efficiency of an office.

5. Reference (b) is modified as follows:

a. Section 29-2.5 is changed to read as follows: "Afloat Exemption. SAs who serve a qualifying deployed special agent afloat (SAA) tour of at least 150 days (excluding pre-deployment workups) may request a 12-month mobility exemption as early as 60 days from the end of the deployment. Additionally, SAAs can submit their request anytime within the 12 months following the end of the deployment. Regardless of when the request is approved, the effective starting

date of this 12 month mobility exemption is the date the afloat assignment ends as documented in a Personnel Status Report (Loss). The exemption automatically expires 12 months from this date. The SAA mobility exemption, and associated requirements, also applies to SAs who complete a Staff Counterintelligence Officer (SCIO) assignment with a deploying numbered fleet. Requests for the 12 month mobility exemption are to be submitted to Code 10D via the geographical field office which had operational control of the SAA while deployed."

b. Section 29-3.2.a is changed to read as follows: "Special agents will submit their bids for SAA vacancies via their chain of command to Code 10D. Code 10D will prepare a list of qualified bidders for review and selection by CRFO."

c. Section 29-10.13 is deleted.

6. This policy will be incorporated into the next revision of NCIS-1, Chapter 13 Special Agent Career Program and NCIS-1, Chapter 29 Special Agent Afloat Program.

7. Questions regarding this revision can be directed to NCIS_SA_CAREERS@navy.mil.

DISTRIBUTION
NCISHQ: All Directorates and Departments
INFO: WWSSD

APPENDIX (4)

From: fox@noms-a.ncis.navy.mil [mailto:fox@noms-a.ncis.navy.mil]

Sent: Tuesday, May 31, 2011 15:41

To: (b)(6) @ncis.navy.mil

Subject: SSD MSG via NOMS

75276 15:40 20110531 IN:SSDEMAIL #14127 OUT:NCISHQWWSSD #125

GENERAL ADMINISTRATION 31MAY11

FROM: 0000 GEN: 11C-0017

TO: DIST

SUBJ: POLICY DOCUMENT NO. 11-08: (PERSONNEL SUPERVISORY SPECIAL AGENT SELECTION PROCESS (SSA-SP))

REFERENCES
(A) GenAdmin 10D-0036/16Mar10/Subj: Update to NCIS-1, Chapter 13: Supervisory Special Agent Selection Process
(B) NCIS-1, Chapter 13: Supervisory Special Agent Selection Process (SSA-SP)/Mar08

1. This Policy Gen Admin document cancels reference (a), and revises reference (b), which sets forth the selection process for supervisory special agents (SSAs).

2. In 2010, the Supervisory Special Agent-Selection Process (SSA-SP) underwent extensive changes as reflected in reference (a). Upon further consideration, the Director, NCIS has decided that the SSA-SP process for FY-11 will include a Phase II oral board interview. The following describes the SSA-SP, to include the new Phase II requirements.

3. The SSA-SP Phase I:

a. The SSA-SP is open to all civilian special agents who have at least five years of qualifying experience as a criminal investigator, or five years as a credentialed military special agent with a military criminal investigative organization, or a combination of service thereof. The five years of experience must include at least three years as a special agent or credentialed military special agent with NCIS. The cut-off date for qualification determination is the date the SSA Headquarters (HQ) review board is scheduled to commence. In order to qualify for the special law enforcement retirement provisions, special agents must have occupied a primary law enforcement officer position (i.e., non-supervisory 1811 position)

for three years before moving to an SSA position.

b. The SSA-SP is initiated with the release of a Gen Admin. Eligible civilian special agents may apply for the SSA-SP by doing the following:

(1) notify their respective Special Agent in Charge (SAC) or Deputy Assistant Director (DAD) of their request for consideration, (2) after notification of the SAC/DAD, submit a career synopsis form and the last three performance evaluations via e-mail to NCIS_SA_Careers@navy.mil requesting consideration, and (3) provide a copy of the career synopsis to their SAC/DAD. The career synopsis form is posted on the HR Directorate webpage at: http://infoweb.ncis.navy.mil/agency/deptwebsites/personnel/documents/opprojs/careersynopsis.doc. The career synopsis provides information regarding the candidate in the following categories: assignment history, deployments/special agent afloat tours/TDYs, academic achievements, awards, and significant career accomplishments.

The information must be provided in descending date order starting with the current position, and may not exceed two pages. All content must be in Times New Roman, 12 font size. The Career Synopsis form located on the NCISnet is the only acceptable form.

c. In consultation with their local leadership teams, SACs/DADs shall complete a SAC/DAD SSA-SP Assessment form for each candidate within their AOR. SACs/DADs will use this evaluation to indicate whether the candidate does or does not possess the necessary competencies and leadership skills to assume an SSA position and to clearly, concisely, and accurately describe the candidate's readiness for management in each of the areas listed in paragraph 3.e. below. Additionally, the SACs/DADs will use the "Comments" section to clearly describe the candidate's suitability for independent assignments and/or assignments in a field office. Also to be addressed in this section is a comment on the candidate's performance since the last formal performance appraisal. This section may also be used for general comments and ranking of the candidate versus other candidates under the leadership of the SAC or DAD.

The SAC/DAD SSA-SP Assessment form is posted on the HR Directorate webpage at:

http://infoweb.ncis.navy.mil/agency/deptwebsites/personnel/documents/opprojs/ssa-sp-assessform_sacdad.doc.

d. The HQ SSA-SP review board will convene, chaired by an SES (or equivalent), with membership consisting of two senior managers at the GS-14/15 level. The board will review each candidate's Selection Consideration File (SCF). The SCF will contain copies of the candidate's last three performance evaluations, the SAC/DAD SSA-SP Assessment Form, and the candidate's Career Synopsis. No other records or files will be reviewed by or made available to the review board. Board members will use the HQ Board SSA-SP Assessment form to evaluate each candidate's SCF and not their personal knowledge of the candidate. Scoring will be in whole numbers only. The HQ Board SSA-SP form is posted on the HR Directorate webpage at:

http://infoweb.ncis.navy.mil/agency/deptwebsites/personnel/documents/opprojs/ssa-sp-assessform_hq.doc

e. Board members will evaluate candidates in Phase I and II on the following competencies:

(1) NCIS Mission Awareness. The candidate is knowledgeable of the mission and organization of NCIS, including an understanding of how the organization fits into the Department of the Navy (DON) and Department of Defense (DoD) at the field office and tactical level. The candidate is conversant in the mission, structure, and responsibilities of NCIS elements at the field office level.

(2) Interpersonal Skills. The candidate considers and responds appropriately to the needs, feelings, and capabilities of different people in different situations; is tactful, compassionate, and sensitive; and treats others with respect. The candidate exercises good judgment by making sound decisions and perceives the impact and implications of decisions.

(3) Oral/Written Communications Skills. The candidate makes clear, convincing oral presentations to individuals or groups, listens effectively and clarifies information as needed; facilitates an open exchange of ideas, and fosters an atmosphere of open communication. The candidate conveys written facts and ideas in a clear, convincing and organized manner.

(4) Technical Credibility. The candidate demonstrates investigative and operational acumen, and possesses knowledge of fundamental aspects of NCIS mission areas. The candidate has been exposed to and understands a broad range of duties such as evidence custodian, EEE custodian, victim/witness coordinator, classified material controls, etc. The candidate appropriately applies procedures, requirements, regulations, and policies related to NCIS field operations.

(5) Leadership. The candidate demonstrates potential to lead with passion, not provocation, and potential to inspire the workforce. The candidate exhibits moral courage, and does the right thing for the right reason and is willing to be held accountable. The candidate demonstrates and promotes values through her or his actions. The candidate strives for balance in all that she or he does. The candidate had a successful tour as a FLETC Counselor, Field Training Agent, Acting SSA, or other performance indicating leadership potential.

f. Scores will be based on the following scale and are defined as:

(1) Outstanding - 5 Points: The candidate's proficiency is expert in this area. The candidate applies the competency in multiple situations without guidance and can train others on this competency.

(2) Excellent - 4 Points: The candidate's proficiency is extensive in this area. The candidate exhibits extensive knowledge of the competency and applies the competency with little or no guidance.

(3) Satisfactory - 3 Points: The candidate has applied this competency in multiple situations and assignments. The candidate applies this competency with some guidance.

(4) Poor - 2 Points: The candidate has difficulty demonstrating this competency due to limited knowledge and/or experience.

(5) No Rating - 0 Points: The candidate displays no proficiency in the competency.

g. When each board member has rated all candidates, the scores for each candidate will be annotated on a composite rating form. The Board Chair will review the composite rating scores. There can be no more than one point difference between board members on any one competency per candidate. The board must resolve a point discrepancy of two points or more. If such differences cannot be resolved after discussion, the assessment form must be fully documented by the board members in question.

h. The candidates will be ranked in order of their summed scores. The board members will then reach consensus on the number of candidates to progress forward to the board interview by identifying a natural break in the scores. In reaching this recommendation, board members will give consideration to the number of anticipated vacancies to be filled, the number of candidates, the range of scores, and the point spread.

i. The Chair and board members will meet with the Deputy Director to discuss the recommended number of candidates who should progress to the board interview. Names will not be provided to the Deputy Director until after the cut-off score has been determined.

j. Upon the Deputy Director's approval, a Gen Admin will be released, announcing the names of the candidates referred to the board interview Phase II.

4. The SSA-SP Phase II will be conducted as follows:

a. The HQ SSA-SP Review Board will interview each candidate using job related and objective questions that will assess the candidate's readiness to assume a position of higher responsibility and authority based on the competencies stated in subparagraph 3.e above.

b. Candidates will receive a single score from each of the three board members based on the scale in paragraph 3.f. The phase II scores will be totaled and then added to the phase I score to obtain the overall rating.

c. At the conclusion of the board interviews, the board members will review the scores without names and determine a natural break in the scores to identify the "best qualified" candidates to be placed on SSA-SP. In identifying a natural break, consideration is given to the number of anticipated vacancies to be filled, the range of scores, and the point spread.

d. The Inspector General (Code 00I) and the Employee Relations Specialist (Code 10A2) will review the recommended selections to identify any selected candidate who has relevant disciplinary action or information contained in internal investigative reports that may bear upon the candidate's ability to perform effectively in an SSA position. The selecting official will weigh the employee's qualifications together with the information provided by Codes 00I and 10A2 in making a final selection decision.

e. The Board Chair serves as the selecting official. The Deputy

Director will serve as the approving official. The selecting official and board members, if available, will meet with the approving official to discuss their recommended number of candidates who should be selected for the SSA-SP. Names will not be provided to the approving official until after the appropriate number of candidates has been determined. Upon approval, a Gen Admin will be released announcing the names of the candidates selected for the SSA-SP.

5. All NCIS selection processes are based on merit. They are conducted without regard to race, color, religion, gender, national origin, age, marital status, or non-disqualifying physical or mental disability, or prior participation in any EEO protected activity. Selections are based on job-related criteria and not on favoritism, personal relationships, nepotism, or patronage.

6. This policy will be incorporated into the next revision of NCIS-1, Chapter 13 Special Agent Career Program.

7. Questions can be directed to Code 10D via e-mail (NCIS_SA_CAREERS@navy.mil).

DISTRIBUTION
NCISHQ: All Directorates and Departments
INFO: WWSSD

FOR OFFICIAL USE ONLY
PAGE 5 LAST (b)(6)

APPENDIX (5)

281506 13:09 20111229 IN:SSDEMAIL #67501 OUT:NCISWWSSD #307

GENERAL ADMINISTRATION 29DEC11

FROM: 0000 GEN: 11C-0044

TO: DIST

SUBJ: POLICY DOCUMENT NO: 11-26: ADMINISTRATIVE (SPECIAL AGENT PERIODIC PHYSICAL EXAMINATION REQUIREMENTS)

REFERENCES

(a) NCIS 1, Chapter 13, Special Agent Career Program/Mar08
(b) NCIS 1, Chapter 46, Recruitment, Screening, and Selection of Special Agents/Dec06

1. The purpose of this policy Gen Admin is to revise reporting requirements and roles and responsibilities of the special agent (SA) and field operations support officer (FOSO) for the management of the required SA periodic physicals contained in references (a) and (b).

2. SAs have an affirmative duty to comply with the requirements of references (a) and (b). Failure to comply may result in disciplinary action. Periodic SA physical examinations are necessary for certifying that the SA is physically capable of performing arduous physical duties without hazard to the SA or others, and will be conducted within 30 days before or after the SA's birthday at ages 24, 27, 30, 33, 36, 38, 40, and annually after the age of 40.

3. The following changes to references (a) and (b) are effective immediately:

a. All previous paper forms for recording the results of SA physical examinations (to include the SF 600 Record of Medical Care) have been replaced in Navy medical facilities by an online system called PC Matrix. PC Matrix includes all of the information necessary to perform the SA physical evaluation. Navy medical providers record the results of the physical exams directly in PC Matrix.

b. A single form, "Physician's Written Opinion," (PWO) is produced by PC Matrix upon completion of the physical, and will be provided to the SA to document the results of the physical evaluation. The form, signed by the medical provider, indicates whether the SA is physically or not physically qualified to perform SA duties and contains no other medical data. A copy of the PWO will also be mailed to Code 10D by the Navy medical facility.

c. Code 10D is responsible for updating TWMS confirming the SA's compliance with the requirements of references (a) and (b).

d. FOSOs and Headquarters office managers are no longer required to mail a copy of the periodic physical certification to NCIS headquarters.

29DEC11

SUBJ: POLICY DOCUMENT NO: 11-26: ADMINISTRATIVE (SPECIAL AGENT PERIODIC PHYSICAL EXAMINATION REQUIREMENTS)

e. FOSOs and Headquarters office managers will continue to ensure SAs complete their periodic physicals per references (a) and (b).

f. SAs are responsible for initiating and attending the examinations at the required times.

4. The changes contained in this policy will be incorporated into the next scheduled revision of NCIS 1, Chapters 13 and 46.

5. The point of contact for this document is, (b)(6) Human Resources, Leadership Development Program (b)(6) or (b)(6) @navy.mil.

DISTRIBUTION:
NCISHQ: All Directorates and Departments
INFO: WWSSD

APPENDIX (6)

325635 14:43 20120209 IN:SSDEMAIL #78246 OUT:NCISWWSSD #412

GENERAL ADMINISTRATION 09FEB12

FROM: 0000 GEN: 11C-0004

TO: DIST

SUBJ: NCIS POLICY DOCUMENT 12-03 PERSONNEL (SUPERVISORY SPECIAL AGENT SELECTION PROCESS (SSA-SP)

REFERENCE
(A) NCIS-1, Chapter 13, Supervisory Special Agent Selection Process (SSA-SP)/Mar08

1. This Policy Gen Admin document revises Appendix (4) in reference (a), which sets forth the selection process for supervisory special agents (SSAs).

2. Appendix (4), paragraph 3.d is changed to amend the SSA-SP PNB membership structure as follows: "The HQ SSA-SP review board will convene chaired by a GS-15, with membership consisting of two senior managers at the GS-14/15 level."

3. All other provisions of paragraph 3.d remain the same.

4. Questions can be directed to Code 10D via e-mail (NCIS_SA_CAREERS@ncis.navy.mil).

DISTRIBUTION
NCISHQ: All Directorates and Departments
INFO: WWSSD/AFLT

APPENDIX (7)

435293 10:32 20121024 IN:SSDEMAIL #103179 OUT:NCISWWSSD #688

GENERAL ADMINISTRATION 24OCT12

FROM: 0000 GEN: 11C-0021

TO: DIST

SUBJ: NCIS POLICY DOCUMENT 12-12: ADMINISTRATIVE (SPECIAL AGENT CAREER PROGRAM - MOBILITY)

REFERENCE
(A) NCIS-1, Chapter 13, Special Agent Career Program of Mar 08

1. Reference (a) is revised. The following policy changes are effective immediately:

a. Section 13-12i(3)(c), the "Pregnancy Deferment" section is changed to read as follows: "A special agent (SA) selected for transfer who is pregnant, or a special agent whose spouse is pregnant, shall, upon request, have their transfer deferred if the report date for the new assignment falls within the third trimester of their pregnancy. The deferment will be in effect until the child reaches three months of age. Likewise, a special agent who has a newborn will be eligible to have a transfer deferred until the child reaches three months of age. If a special circumstance exists requiring a deferment beginning sooner than the third trimester of pregnancy or lasting beyond three months after birth, a request must be submitted via the humanitarian/hardship (H/H) procedure. Upon expiration of the deferment, the SA will be expected to be available for transfer as determined by the needs of the agency."

b. Section 13-14b, the last sentence of this section is changed to read as follows: "With this in consideration, selected or unrequested transfers may occur to satisfy the needs of the service."

c. Section 13-15e(1), the "Humanitarian/Hardship Requests" section is modified to include the following as the last sentence to the paragraph: "Employees are strongly encouraged to submit their H/H request as soon as they have reason to believe that they have a severe personal hardship which impacts their mobility. Barring unique circumstances, NCIS will not consider H/H requests which are submitted subsequent to selection for PCS unless the applicant provides clear and compelling reasons for why the agency did not receive prior notice."

d. Section 13-15e(2), the "Humanitarian/Hardship Factors" section is changed to include the following as paragraph (g): "The problem/situation is of a finite duration."

e. Section 13-15e(4)(a) is changed to read as follows: "For financial or business reasons (including the operation of a family business or loss of home value)."

f. Section 13-15e(5)(a)3d is changed to read as follows: "H/H requests granted due to unsuitability of applicant or applicant's family members in one or more OCONUS locations are based on factors specific to the locations identified and will not necessarily preclude the transfer of the applicant and family members to other OCONUS locations or CONUS assignment."

2. This policy document will be appended to NCIS-1, Chapter 13 until the revision is released.

3. Questions regarding this chapter update can be directed to NCIS_SA_CAREERS@ncis.navy.mil.

DISTRIBUTION
NCISHQ: All Directorates and Departments
INFO: WWSSD

Pages 220 through 280 redacted for the following reasons:
- -
(b)(7)(E)

CHAPTER 14
TITLE: EMPLOYEE TRAINING AND DEVELOPMENT
POC: CODE 10B
DATE: DEC 06

14-1. GENERAL

14-1.1. This chapter promulgates policy and procedures regarding employee development at the Naval Criminal Investigative Service (NCIS). This ensures that all personnel have the opportunity to participate in a comprehensive employee development program throughout their careers to meet and support current and emerging NCIS missions. Central administration and control of the NCIS employee development program by the NCIS Training Academy (Code 10B) is essential for effective use of available resources and maintain a flexible posture to meet emerging, identified, and validated training needs.

14-1.2. References

a. Department of Navy (DON) Civilian Human Resources Manual (CHRM) Subchapter 410.

b. DON Office of Civilian Human Resources Memorandum, Subject: Business Practice Changes for Managing Employee Development, 12 December 2003.

c. Federal Law Enforcement Training Accreditation (FLETA) Professional Training Standards Manual 2005.

d. Title 5, Chapter I, Part 410, Subpart D, Sec. 410.404 - Determining if a conference is a training activity, revised as of January 1, 2002.

e. SECNAVINST 5212.5 (Series), Navy and Marine Corps Records Disposition Manual.

14-1.3. A list of acronyms and respective long titles utilized in the text of NCIS-1 Chapter 14 can be found in GLOSSARY OF ACRONYMS.

14-2. MISSION

The mission of the NCIS Training Academy is to serve as the premier provider of training for NCIS employees. The Training Academy (Code 10B) is responsible for providing relevant, timely, substantive, and cost effective training programs while supporting the NCIS Strategic Plan by providing the tools to build a highly skilled workforce. The Academy has responsibility over all basic, advance, and In-Service training programs. All instructional programs will be designed based on the five-step ADDIE (Analyze, Design, Development, Implementation, and Evaluation) method of Instructional Systems Design (ISD).

a. The Deputy Assistant Director (Code 10B) is also recognized as the Director of the NCIS Training Academy, located at the Federal Law Enforcement Training Center (FLETC), Glynco, Georgia. The Academy Director will serve as the NCIS representative to FLETC and FLETC partner organizations.

b. The Training Academy Director is authorized to create and maintain a Training Manual (NCIS-7) that will supersede all previous published guidance, i.e., directives or instructions. The purpose of NCIS-7 is to establish internal administrative policy and procedures for the Training Academy and training within the organization. The manual will ensure training within NCIS is validated and the guiding principles of the FLETA standards are maintained within NCIS Training.

14-3. RESPONSIBILITIES

Comprehensive and effective employee development requires action at all agency and operational levels.

a. Director, Naval Criminal Investigative Service will:

(1) Support and provide resources to advance employee development.

b. Assistant Director (AD), Human Resources Directorate, Naval Criminal Investigative Service will:

(**1)** Maintain the authority to issue, modify, and approve written Training and Employee Development Directives.

(**2)** Support the "training is an investment" concept.

(**3)** Provide resources to execute the Annual Training Plan.

(**4)** Assist in providing data for the NCIS strategic (Five year) training Plan.

c. Deputy Assistant Director (DAD) for Training will:

(1) Establish and maintain a comprehensive training and employee development program. This includes development and implementation of a training program to ensure that all NCIS personnel are capable of performing the functions necessary to enable NCIS to effectively achieve organizational objectives; and,

(2) Will conduct an annual assessment of organizational training needs through workforce planning activities, formal skills assessment, and coordination with management officials to identify performance deficiencies that are skills related and a periodic evaluation of changes in skill requirements; and,

(3) Develop and implement the curricula for Special Agent Basic Training (SABT). Additionally, develop and deliver training to address those needs through available training tools and delivery methods to include training provided directly at FLETC or at other locations provided by NCIS, DON, or government institutions, use of outside vendors either in a group setting, or, on an individual basis, and use of e-learning tools.

(4) Responsible for coordinating with management to develop and provide ongoing employee development program that will enhance employee performance, motivation and competitiveness and lead to improved capacity to achieve organizational objectives.

(5) Will provide for continual assessment and refinement of training strategies and delivery methods in collaboration with other NCIS entities to ensure training is effective, timely and is reaching the right audience. Specific training functions are described below.

(6) The DAD is responsible to ensure an effective SABT program is provided new special agents with the requisite basic knowledge, skills and abilities. This involves continued monitoring of the existing course content and development of new course to ensure the changing needs of the organization are being addressed. Critical to the success of the SABT program is the process to provide an assessment of new special agents, in the training environment, as well as monitoring their progress in the field. The

DAD will ensure all courses and training developed for the SABT will be delivered by qualified instructors and meet the standards for training certification.

(7) Advance Special Agent Training: The DAD will be responsible to develop/acquire and deliver advanced investigative and operational courses that meet the prioritized needs of the operational program. The program must provide experienced investigators with necessary training to keep their skills and abilities at the level required to be effective in the performance of their duties. The DAD will coordinate with all operational programs to insure the organization priorities and needs are being met.

(8) Professional and Support Staff Development: The DAD is responsible for addressing job related training needs, specialized training and career development needs for all professional and support staff (non-special agent employees). The NCIS Professional and Support Staff training programs will be based on the assessment of staff skill and knowledge requirements to perform specific duties and responsibilities.

(9) Training Needs Assessment: The DAD is responsible for ensuring that training function activities are based upon formal assessment of all levels of personnel within the organization. In order to meet the requirements, the program will conduct an annual Training Needs Assessment, one that encompasses all Field Offices' and Headquarters' activities, to determine training requirements necessary to meet all operational and support program priorities. The Training Needs Assessment will also serve as a resource document to support training budgeting and planning activities.

(10) Training Plan: The DAD is responsible for developing the NCIS Training Plan. The Training Plan will reflect both short and long term training initiatives (six-year), annual training plan/schedule, and budget requirements necessary to satisfy NCIS training needs identified in the Training Needs Assessment. The DAD will coordinate development of the training plan and all operational and support programs. The Training Plan will be updated annually to reflect changes in priorities and assessed needs.

(11) Maintain the authority to issue, modify, and approve written Training and Employee Development Directives. To ensure that all Training Directives are maintained, indexed, purged, updated, and revised according to current DON and FLETC Accreditation policies, instructions, standards, and guidelines.

(12) Ensure that all statements of policy, rules, regulations, and procedures for executing all training covered by this Chapter are reviewed and maintained by the DAD for Training. Develop and issue manual NCIS-1 Chapter 14 changes that impact NCIS policy.

(13) Ensure all training directives are posted, distributed, stored, and backed-up via NCIS Intranet architecture, according to current NCIS Information Resource Management and NCIS Human Resources Directorate guidance. Computerized documentation will provide 24-hour just-in-time accessibility, and will be the primary

means of storage, dissemination and maintain a receipt-acknowledged database on all directive and/or policy updates related to training.

(14) Review and comment on all Navy Training Plans that may impact training of NCIS personnel.

(15) Develop, staff, and submit budget requirements for centrally managed employee development of NCIS personnel. Manage and execute funds received in support of the submitted training requirements.

(16) Provide technical direction, guidance, and support to Field Instructors, Field Training Agents (FTA), Field Training Coordinators (FTC) and HQ Training Coordinators (HTC). Ensure that instructors have completed the Field Training Evaluator Program (FETP).

(17) Identify and disseminate information regarding training opportunities to all elements of NCIS.

(18) Control, provide oversight, and approve all training, initiatives, and liaison with training centers and/or departments of counterpart agencies with centrally managed training funds. Included are counterpart agencies such as the Federal Bureau of Investigation, U. S. Army Criminal Investigative Division/Military Intelligence, U. S. Air Force Office of Special Investigations, Joint Counterintelligence Training Academy. Additional training, or, educational facilities include Seat-Of-Government sponsored FLETC, Defense Intelligence College, Defense Polygraph Institute, Naval War College, Naval Post Graduate School, and the Department of Defense Security Institute.

(19) Develop an Annual Training Plan based on consolidated input from the AD, DAD, SAC personnel, and the Annual Needs Assessment.

(20) Publish a monthly Situation Report (SITREP) providing up-to-date information on the status of the NCIS Training Department to NCIS senior management and executive staff.

(21) Ensure any subcontracted NCIS Training Academy programs meet accreditation directives.

(22) Oversee the input and support of manual and or automated Training Record Documentation. Automated training files support effective agency wide auditing and training completion tracking. Training records will be maintained in the most current NCIS, DON, or OPM provided databases, i.e., Defense Civilian Personnel Data System (DCPDS).

(23) All mandatory training, regardless of length, will be documented. All training consisting of eight (8) hours, or, more, will also be documented following validation by the Training Academy.

(24) Develop and maintain written directives that establish guidelines for all Academy developed training on:

(a) Instructor – Student ratio.
(b) Support Staff – Instructor ratio.
(c) Instructor preparation times.
(d) Updating lesson plans.
(e) Monitoring instruction.
(f) Instructor qualifications.
(g) Curriculum development, approval, and review.
(h) Records Maintenance.

d. The DADs and SACs will:

(1) Ensure newly hired personnel receive initial indoctrination (orientation) and in-processing as discussed in ADDENDUM 1.

(2) Implement and manage the Field Training Agent Program FTAP), including records management as discussed in ADDENDUM 2.

(3) Implement and manage the In-Service Training Program for all personnel assigned to the Field Office/HQ Codes, including records management as discussed in ADDENDUM 3.

(4) Recommend qualified employees for training to the Training Academy.

(5) Submit quarterly and special training requirements to the Training Academy.

(6) Administer in-service training, and ensure that all training be coordinated with Training Academy staff.

(7) Review policies and instructions with the Training Academy that may impact personnel training.

(8) Ensure compliance with completion and submission of Individual Development Plans (IDP).

(9) Review IDPs, and submit recommendations for improvements.

(10) Designate an HTC for the following HQ Codes 10, 11, 12, 14, 15, 21, 22, 23, 24, and 25.

e. FTC/HTC designees will:

(1) Administer the Pre-Basic Special Agent Orientation Program (Phase I) as discussed in ADDENDUM 1.

(2) Manage and implement the FTAP as discussed in ADDENDUM 2.

(3) Maintain hard copies of all Training Directives to support potential Intranet failures.

(4) Ensure that all mandatory training is documented according to current NCIS policy.

(5) The results of all mandatory In-Service Training accomplished by the personnel in the field offices and at NCIS Headquarter's codes will be submitted to the Training Academy by the FTCs and/or HTCs on a quarterly basis. Reports will be submitted within 15 days following the end of the previous quarter. FY quarters are identified as October-December; January-March; April-June; and July-September.

f. Employees:

(1) Employees share responsibility for their individual career development with their supervisors and the Training Academy. Employees should familiarize themselves with the DON Civilian Human Resources Employee Development guidelines.

(2) Requests for training must be submitted to the Training Academy (Code 10B) at least 21 days before the start of class. At no time is an employee permitted to attend training funded, or, administered by, the Training Academy without receiving prior approval of the Training Academy.

(3) Supervisors who have nominated employees that will be unable to attend training classes must notify the Training Academy (Code 10B) in advance of the schedule training. In an effort to conserve limited resources, any cancellation request should be made at least two-weeks prior to the start date of the training and should include sufficient justification regarding that individual's inability to attend the selected training.

14-4. TRAINING PROGRAMS

14-4.1. All Employee Development initiatives, training, on-the-job training, self-development, etc., fall within the scope of the Training Academy. Course development and content is the responsibility of the Training Academy and will be in full compliance with the FLETA. The academy will seek and utilize Subject Matter Experts (SME) to develop programs; however, the Training Academy is responsible for the curricula and training delivery method.

14-4.2. Training opportunities will be announced to all employees by the publishing of a quarterly training calendar with additional posting to the Training Academy website. The quarterly training schedule will provide available training courses for that quarter with a short description, date and location of the training. This will permit the SACs and DADs time to nominate employees for training opportunities well in advance of the training and ensure their workforce has the competency able to meet mission requirements. Nomination and selection information will be retained according to SECNAVINST 5212.5 (series). The selection of nominees is the responsibility of the Training Academy.

14-4.3. Employees attending Academy sponsored training programs fall under the Academy supervisory authority during the period they are in a training status. The Training Academy supervisory staff will approve/ disapprove all requests by students to be excused from portions of on-going training classes. The Training Academy will provide feedback to the employee's Rater of Record regarding performance issues that may arise during training. Individuals that successfully complete the training will receive a "CERTIFICATE OF TRAINING" and their training file will be updated. If an individual fails to successfully complete any advanced training program the Training Academy Director has the option of giving the individual a "CERTIFICATE OF ATTENDANCE" and their training file will be annotated as appropriate, or, the individual will be totally removed from the training program. Successful completion of testable training programs requires a score of 70% or higher.

14-4.4. The supervisor's employee is responsible to submit an IDP to the Training Academy for processing. The employee, working closely with their supervisor, will identify skills sets that are needed by the employee. Once desired skills sets are identified by the supervisor and employee, an appropriate method to obtain them will be selected. Training which compliments on-the-job development is in the best interest of individuals, supervisors, and the NCIS. If a training program is the appropriate method, the Training Academy will take for action to find and schedule training for the employee.

14-4.5. The Training Academy will fund employee attendance at conferences when it is relevant to improving individual and/or organizational performance and developmental benefits will be derived through the employee's attendance. (SOURCE: 5 CFR 410.404 and CPI 410.8-1, CPM 410.3-5.) Additionally, the conference must meet the following criterion:

a. The announced purpose of the conference is educational or instructional; and/or,

b. More than half of the time is scheduled for a planned, organized exchange of information between the presenters and the audience which meets the definition of training in Section 4101 of Title 5, United States Code; and/or,

c. The content of the conference is germane to improving individual and/or organizational performance; and/or,

d. Development benefits will be derived through the employee's attendance.

e. Conferences not meeting the above criteria should be budgeted and funded by cognizant field offices or departments.

14-4.6. The Training Academy is responsible for the establishment and maintenance of a comprehensive training and employee development program. The Training Academy will develop and implement the curricula for Special Agent Basic Training (SABT). Additionally, they will develop and deliver training to address those needs through available training tools and delivery methods to include training provided through a variety of locations and vendors. This training will enhance employee performance, motivation, and competitiveness, and lead to improved capacity to achieve organizational objectives. Specifics can be found in Addendum 1 and at the Training Academy Website.

a. Special Agent Basic Training (SABT) - The Training Academy is responsible to ensure an effective training program to provide new special agents with the requisite basic knowledge, skills and abilities. This involves continued monitoring of the existing course content and development of new courses to ensure the changing needs of the organization are being addressed. The ability to provide an assessment of new special agents, both in the training environment as well as monitoring progress in the field, is critical to the success of the program. This training consists of four-phases which are:

Phase I – Pre-Basic Special Agent Orientation at the NCISFO/HQ departments prior to going to formal training at the FLETC.

Phase II - Formal training at FLETC to include both the Criminal Investigator Training Program (CITP) and SABT.

Phase III - The FTAP begins upon graduation from FLETC. Phase III is the on-the-job-training (OJT) portion of the FTAP.

Phase IV – Upon completion of Phase III, an evaluation will be made whether the Training Agent should remain in Phase III mode or move into Phase IV (final evaluation of case work and abilities.) Phase IV begins if the TA successfully completes all the skill requirements and all evaluations are at an acceptable level. Phase IV lasts until the successful completion of the trial period.

Graduation from CITP/SABT and completion of all phases is a requirement for successful completion of the special agent trial period. Each phase is discussed in more detail in ADDENDUM 2.

b. Advanced Special Agent Training – Any course taken after graduation from the SABT. The Training Academy is responsible to develop/acquire and deliver advanced investigative and operational courses that meet the prioritized needs of the

operational programs. Advanced Special Agent training courses provide the employee with the technical skills and knowledge required at a journeyman level keeping the special agent effective in the performance of their duties. NCISFO SACs have a responsibility to inform NCISHQ Program Managers of skills sets and competency levels required of their workforce for them to meet mission requirements. NCISHQ program manager are responsible for coordinating this information with the Training Academy staff to ensure appropriate training program are developed to meet mission requirements.

c. Professional and Support Staff Development – The Training Academy (Code 10B) is responsible for addressing job-related training needs, specialized training, and career development needs for all professional and support staff. This category is intentionally broad and encompasses a variety of training to meet the Agency's needs in areas such as: computer, finance, equal employment opportunity (EEO), effective briefing, analysis, legal, information management, etc. As resources permit, developmental training (i.e. cross-training) and self-development opportunities are encouraged.

d. Correspondence Courses – There is a wide variety of correspondence courses that employees are encouraged to pursue. These courses should have a relationship to current or future duties that will assist in broadening the background and knowledge of the employee. This category includes on-line training offered by the Navy Knowledge Online (NKO), accessed through NKO Login.

e. In-Service Training is developed and managed by the Training Academy. The training will be standardized and presented each quarter. NCISFO/HQ codes are responsible for the implementation of this program within their respective subordinate offices. Special agents will receive a minimum of eight hours of general investigative topics, less local discretionary training. Professional and support personnel are encouraged to attend appropriate In-Service Training. The specifics of the program can be found at ADDENDUM 3.

f. The FTAP is developed and managed by the Training Academy. The FTAP formalizes the professional training and guidance a special agent receives during his/her trial period. U. S. Marine Corps Special Agents are included in the FTAP. Field Offices are responsible for the implementation of this program within their AOR . Subordinate offices will administer the FTAP program at the local level under the supervision of the FTC or SAC designee. The specifics of the program can be found in ADDENDUM 2.

g. The NCIS Tuition Assistance Program (TAP) provides employees the opportunity to apply for tuition assistance for mission related courses at an accredited college or university. The basic objective of the TAP is to encourage and assist employees to increase their knowledge, skills and abilities in order to perform the duties of their current position and strengthen their potential contribution to the overall mission of the agency. The specifics of the program can be found in ADDENDUM 9.

14-5. RECORDING TRAINING ACCOMPLISHMENTS/REQUESTS

14-5.1. SECNAVINST 5212.5 (series) provides details and guidance for required reporting and retention of training data.

14-5.2. Some training topics are considered to be DON Mandatory/Recurring Training Requirements (MRTRs). Those topics are located in ADDENDUM 7. It is required that this training is recorded in the current NCIS Training Documentation Database.

14-5.3. Training that is mandatory, or, greater than 8-hours in duration and approved by the Training Academy, is considered formal training and will be documented in employee's training files. Training files may be automated, or, hard copy, supporting effective agency wide audit and tracking the completion of training. Training records shall be maintained in the most current NCIS, DON, and or OPM provided training documentation databases. Currently the Training Academy inputs training records into the DCPDS. Employees may monitor their own shadow training file; however, the Training Academy database is considered the official training file.

14-5.4. The reporting of all formal training is the responsibility of the FTC to include training not coordinated or funded by the Training Academy. Reporting of all formal training coordinated or funded by Code 10B will be the responsibility of the Training Academy staff. If the current Training Documentation Database is not locally accessible by the FTC the input will be accomplished by the Training Academy. It is a FTC responsibility to ensure the Training Academy has the data necessary for input.

14-5.5. Reporting of educational endeavors pursued by employees on their own time, on a voluntary basis, such as various adult education continuation programs, and/or college level courses, may be submitted to the Training Academy. The Training Academy will review the submitted information and determine applicability for input to the current Training Documentation Database.

14-6. TRAINING PROVIDED TO FOREIGN POLICE AGENCIES

14-6.1. The Arms Export Control Act, 22 U.S. Code, Section 2751, places limits on the export of "Defense Services." Police training is a "defense service" that may only be conducted under the Foreign Military Sales/Security Assistance Program provided the consumer country pays for the training and the Defense Security Assistance Agency (DSAA) approves the sale of the "defense service". Requests for such training assistance to foreign police agencies will be submitted to the NCIS Training Academy.

14-6.2. NCIS components may, without prior approval conduct familiarization briefings with foreign police agencies provided such activity is directly related to the NCIS mission in the foreign country. For example, joint familiarization regarding Protective Service Operation (PSO) procedures in anticipation of a protected principal visit to that country; detailed briefings and/or rehearsals regarding narcotics suppression operations; or briefings/familiarization regarding investigative procedures where joint investigations are conducted are authorized and no prior coordination is required.

14-7. LOCAL DISCRETIONARY TRAINING

14-7.1. On occasion, training opportunities not provided by the Training Academy are identified by NCIS field components. If the field component chooses to fund this training, all actions required, including entry of course completion in to the current Training Documentation Database are the responsibility of the field component. Upon completion of the training, the Training Academy requires a critique of the course(s).

14-7.2. If a field component identifies a need for training that is not provided by the Training Academy, a request for that training may be submitted to the Training Academy using the Training Request form found on at NCISnet-TRAINING . If the training is approved then all actions required for attendance will be the responsibility of the Training Academy.

14-8. GLOSSARY OF ACRONYMS

ACRONYM	LONG TITLE
AD	Assistant Director
ADDIE	Analyze, Design, Development, Implementation, Evaluation
CHRM	DON Civilian Human Resources Manual
CITP	Criminal Investigator Training Program
DAD	Deputy Assistant Director
DCPDS	Defense Civilian Personnel Data System
DON	Department of the Navy
FETP	Field Training Evaluator Program
FLETA	Federal Law Enforcement Training Accreditation
FLETC	Federal Law Enforcement Training Center
FTA	Field Training Agent
FTAP	Field Training Agent Program
FTC	Field Training Coordinator
HTC	Headquarters Training Coordinator
IDP	Individual Development Plan
NKO	Navy Knowledge On-line
OJT	On-The-Job-Training
PSO	Protective Service Operation
SABTP	Special Agent Basic Training Program
SAC	Special Agent in Charge
SITREP	Situation Report
SME	Subject Matter Experts
TAP	Tuition Assistance Program

Pages 294 through 357 redacted for the following reasons:
- -
(b)(5)

CHAPTER 15
TITLE: HOURS OF WORK, PAY, AND LEAVE
POC: CODE 10A
DATE: MAR 09

POLICY DOCUMENT
APPENDIX (3) Gen Admin 11-0031 of 2 Sept 2011 released NCIS Policy Document No. 11-17: Administrative (Hours of Work). Policy Document 11-17 contains revised or new policy that has been incorporated into this chapter and should be reviewed in its entirety.

APPENDIX (4) Policy Document 14-01: Administrative (Law Enforcement Availability Pay – LEAP)

15-1. INTRODUCTION

15-1.1. This chapter establishes the requirements and procedures for assigning and approving the hours of work, rates of pay, and use of leave for employees of the Naval Criminal Investigative Service (NCIS). These procedures comply with the requirements of Title 5 United States Code (USC) Chapters 53 (Pay Rates and Systems), 55 (Pay Administration), 59 (Allowances), 61 (Hours of Work) and 63 (Leave). This policy also complies with the commensurate sections of Title 5, Code of Federal Regulations (CFR) and Department of Defense (DoD) and Department of Navy (DON) instructions and directives.

15-1.2. Answers to frequently asked questions regarding pay and leave may be found at the Department of the Navy Human Resources website.

15-1.3. This chapter applies to all NCIS employees who meet the definition of employee in Title 5 USC 2105.

15-2. HOURS OF WORK

15-2.1. General information on hours of work may be found at 5 CFR Part 610. Information specific to NCIS is provided below.

15-2.2. Full-Time Work Schedule.

a. The normal workday is 0730-1600. Employees may, with the approval of their supervisor, set work schedules that vary by up to 90 minutes before or after the normal starting time of 0730. Work schedules should remain constant.

b. Supervisors may authorize a Compressed Work Schedule (CWS) if the mission and functions of the immediate organization permit this flexibility. The CWS enables employees to fulfill their basic workweek requirements in less than 10 days during the biweekly pay period. All full-time non-special agent civilian employees may be eligible to participate in the CWS.

(1) The primary objective in establishing the CWS within NCIS is to enhance employee recruitment and retention, reduce parking congestion, reduce overtime expenses and absenteeism, increase productivity, and allow employees the opportunity to improve their job satisfaction and quality of work life, while fully supporting mission accomplishment.

(2) The CWS is offered as a privilege to those employees identified as being eligible. Participation in the CWS is on a voluntary basis; no employee is required to participate in CWS. An employee may participate in the CWS provided that participation does not interfere with effective mission accomplishment or the employee's performance of official duties. Every effort will be made to accommodate an employee's selection of a work schedule option; however, supervisors retain the right to establish or revise any work schedule in order to avoid adverse impact on daily operations.

(3) Temporary Duty (TDY) and Training. When TDY or training is scheduled during the pay period, the employee will normally revert to the basic 8-hour workday, 40 hours per week work schedule for the entire pay period(s) while in a training/travel status. However, if the TDY/training schedule coincides with the employee's CWS tour of duty, the supervisor may permit the employee to remain in a CWS status.

(4) Holidays. When a holiday occurs on a CWS scheduled day off, the preceding workday before the holiday becomes the holiday with the CWS day off remaining the same.

(5) Any day of the workweek, Monday through Friday, may be used as the "off" day in a CWS schedule. Likewise, any day of the workweek may be used as the short (8-1/2 hour) workday. However, the established non-workday and the short day will remain constant each pay period unless operational requirements dictate that the day(s) be changed. Tours of duty under the CWS must fall within the normal scheduling times and therefore must not begin earlier than 0600 nor end after 1800. All schedules must be approved by the employee's supervisor.

(6) Incumbents of certain positions, because of the nature of the work, may be required to remain on a basic workweek schedule (8 hours per day Monday through Friday).

(7) Denial of an employee's request to participate in the CWS is not grievable.

15-2.3. Part -Time Work Schedule.

a. Part-time work schedules enable NCIS to retain highly qualified personnel in both special agent (SA) and professional/ support staff positions, while allowing flexibility for employees to manage other compelling personal situations that might otherwise cause them to terminate their employment. Part-time work schedules usually range from 16 to 32 hours per week. The normal scheduled tour of duty must include at least 4 hours of work on any day identified as a work day and may not exceed 10 hours per day.

b. For professional/support staff, a request to establish a part-time work schedule or to convert from full-time to part-time status should be initiated in writing by an employee and submitted to his or her supervisor. Employees may request a part-time work schedule for a temporary period of time or as a permanent measure. The appropriate special agent in charge (SAC) or deputy assistant director (DAD) may approve part-time work schedules.

c. Part-time employment for SA personnel requires the development of a more formalized program referred to as the Part Time Agent Program (PTAP). PTAP assignments will be established for a minimum of 6 months and a maximum of 1 year.

d. In order to qualify for a PTAP assignment, the SA must:

(1) Demonstrate a compelling personal need, i.e., child care, elder care, death of/or dying spouse or other close family member, or illness which might otherwise cause the employee to resign in order to deal with the situation or severely impact the employee's ability to fulfill the obligations of full-time employment,

(2) Have served as a special agent for a minimum of 2 years,

(3) Have received a rating of "pass" for the last two annual appraisal periods.

e. To apply for conversion to the PTAP, a SA must provide a detailed memorandum to the SAC or DAD requesting permission to participate in the PTAP. The application must state the reason(s) for entry into the program and certify that the SA meets all the qualifications. The request must indicate the proposed number of hours per week and include a tentative bi-weekly schedule.

f. Authority to approve participation in the PTAP and the continuation or extension of an assignment is delegated to the DAD for Personnel Operations and Services, Code 10A. Recommendations to approve, disapprove, extend, or terminate PTAP assignments will be initiated by the appropriate SAC or DAD and include an assessment of the impact on the office of the loss of the full time services of the SA.

g. Requests for less than 6 months should normally be handled through the use of the voluntary leave transfer program, if applicable, or the use of leave without pay (LWOP).

h. Code 10A will advise the SAC or DAD and the affected employee of the decision regarding the request to participate in the PTAP. If approved, Code 10A will update the Defense Civilian Personnel Data System (DCPDS) and the NCIS Human Resources information system to record the change in work schedule. The supervisor is responsible for submitting a revised work schedule to Code 10A2 to ensure the accuracy of the Standard Labor Data Collection and Distribution (SLDCADA) records.

i. If a SA is denied acceptance into the program, denied a requested extension, or removed from the part-time program other than at their own request, they may appeal the action to the Assistant Director (AD) for Human Resources (Code 10). The appeal must be in writing and should address why the decision of the DAD for Personnel Operations and Services may be inappropriate.

j. Work schedules and assignments will be set by the part-time special agent's immediate supervisor with the concurrence of the SAC or DAD, dependent upon the needs of the office and the part-time SA's personal circumstances. Managers will exercise sound judgment, creativity, and resourcefulness in deploying the part-time SA.

(1) For example, a part-time SA may be assigned a full case load and be given additional time to complete the investigations; assigned limited cases; assigned to assist other agents; or, assigned as a task force member.

(2) The success of this program necessitates flexibility and progressive leadership from managers. Likewise, participants in the program must continue to provide high quality performance in support of the mission of their respective office and NCIS.

k. PTAP participants must be advised that certain limited circumstances may require their return to work on a full-time basis. Any request for a change in status must be the result of a change of office resources or circumstances affecting the ability to meet mission requirements.

(1) Failure on the part of the employee to maintain at least a level 3 rating during the part time assignment will be considered sufficient reason to require a return to full-time status in order to more completely evaluate performance.

(2) The SAC or DAD must notify the SA in writing of the reason(s) for the change in employment status. This notification must be provided at least 30 days in advance of the date the employee will be required to return to full-time status.

15-2.4. Unique Work Schedule Situations. When an employee is on a TDY assignment, or otherwise absent from the permanent duty station, he or she may be required to work tours of duty that do not coincide with the tour normally worked. In such situations, it is imperative that the employee communicates the new tour of duty and the actual hours worked to the supervisor. The supervisor, or the designated timekeeper, will submit a tour of duty change, if necessary, to Code 10A2.

15-2.5. Travel. Information on the hours of work for time spent in a travel status may be found at 5 CFR 551.442.

15-3. GENERAL PAY INFORMATION

General information on pay under the General Schedule, including holiday pay, shift differentials, Sunday and other premium pays, can be found at 5 CFR Part 550.

15-4. LAW ENFORCEMENT AVAILABILITY PAY (LEAP)

15-4.1. Purpose of LEAP. The purpose of LEAP is to provide a special premium pay to SAs to ensure their availability for unscheduled duty in excess of a 40-hour work week, based on the needs of the employing agency. SAs will continue to receive LEAP following NCIS' conversion to the National Security Personnel System (NSPS). DoD 1400.25-M, Section SC1930.29 provides that LEAP will continue to be paid under the provisions of Title 5 USC 5545a and 5 CFR 550.181 through 550.187.

a. LEAP is paid to SAs at the rate of 25 percent of basic pay based on their performance of unscheduled duty, and each SA's eligibility to receive LEAP is directly linked to his or her supervisor's certification that the SA has met, or is expected to meet the substantial hours requirement. SAs who are not meeting, or who are not expected to meet the substantial hours requirement, are not eligible to receive LEAP.

b. LEAP continues when an SA is attending NCIS-sanctioned training, on NCIS-ordered travel, on approved leave, or during excused absences.

c. LEAP is considered part of basic pay for the following purposes: advances in pay, workers' compensation, retirement benefits, thrift savings plan, life insurance, and lump sum annual leave payments. LEAP is also considered basic pay for severance pay purposes, and is included in Voluntary Separation Incentive Pay (VSIP) computations.

d. SAs participating in the PTAP are ineligible for LEAP for the duration of their participation in PTAP.

15-4.2. Unscheduled Duty Hours. For the purpose of LEAP, unscheduled duty hours are those hours during which an SA performs work that is not:

a. Part of the 40-hour basic workweek of the SA; or,

b. Regularly scheduled overtime hours compensated under 5 U.S.C. 5542 and 5 CFR 550.111.

15-4.3. Substantial Hours Requirement. SAs are paid LEAP if their annual average of unscheduled duty hours worked in excess of each Regular Workday is equal to or greater than 2 hours. This is called the "substantial hours requirement". Unscheduled duty hours which are worked by an SA on days that are not Regular Workdays are also considered in the substantial

hours requirement calculation. Additionally, the first 2 overtime hours on any day containing part of an SA's basic 40-hour workweek are covered by LEAP, without regard to whether the hours are scheduled or unscheduled, and those hours are also included in the calculation.

a. Calculation of the Substantial Hours Requirement. The substantial hours requirement is calculated by dividing the "Total Unscheduled Duty Hours Worked" (the numerator), by the "Total Regular Workdays" (the denominator). To meet the substantial hours requirement, the resulting quotient must be equal to, or greater than 2.

b. Definition of a "Regular Workday": For the purpose of calculating the substantial hours requirement, a "Regular Workday" means each day in the SA's basic work week during which he/she works at least 4 hours, excluding:

(1) Overtime hours paid under 5 USC 5542; or,

(2) Unscheduled Duty Hours compensated by LEAP; or,

(3) Hours during which an SA is:

(a) Engaged in NCIS-approved training (use appropriate operations code) or non-operational travel associated with training/conferences as defined in Section 15-7; or,

(b) On approved leave; or,

(c) On excused absence with pay (including paid holidays).

15-4.4. Certification Requirements. SAs and their supervisors are required to "certify" an SA's availability for unscheduled duty hours. This certification is documented on the "Certificate of Availability for Unscheduled Duty".

a. Certification of New SAs. Upon hiring, new SAs and their supervisors must certify that the SAs are expected to meet the substantial hours requirement during the upcoming 1-year period.

(1) New SAs are responsible for completing and signing a Certificate of Availability for Unscheduled Duty during the entry on duty (EOD) process.

(2) Supervisors of new SA personnel are responsible for:

(a) Ensuring that the new SA completed and signed a Certificate of Availability for Unscheduled Duty; and,

(b) Validating the new SA's Certificate of Availability for Unscheduled Duty by signing the document and forwarding a copy to the Pay and Entitlements Branch (Code 10A12) within 2 weeks of the new SA's entry on duty.

b. Annual Certification. Each year, SAs receiving LEAP, and their supervisors, must certify that the SAs currently meet, and are expected to continue to meet, the substantial hours requirement during the upcoming 1-year period. The "Certificate of Availability for Unscheduled Duty".

(1) SAs are responsible for preparing a new "Certificate of Availability for Unscheduled Duty" and submitting it to their supervisor not later than 15 January of each year.

(2) Supervisors of SAs are responsible for certifying the availability of each SA under their supervision by ensuring that each SA prepares a new "Certificate of Availability for Unscheduled Duty" and by signing the certificate, indicating that the SA currently meets, and is expected to continue to meet, the substantial hours requirement during the upcoming 1-year period. Once completed, the supervisor is responsible for forwarding a copy of the certifications to Code 10A by 30 January of each year.

(3) Code 10A is responsible for receiving and maintaining a repository of all current SA certifications of availability, including the reporting of and follow-up on certifications not received.

c. Certification of Unavailability for Unscheduled Duty. An SA may request that he or she not be assigned unscheduled duty hours for a designated period of time, because of a personal or family hardship. The "Certification of Unavailability for Unscheduled Duty" will be used to document this request.

(1) SAs are responsible for forwarding their completed "Certification of Unavailability for Unscheduled Duty" to their supervisor immediately upon realizing that a personal or family hardship will make them unavailable for unscheduled duty.

(2) The supervisor is responsible for reviewing and validating the request and forwarding it to the appropriate SAC/DAD for final approval.

(3) The SAC/DAD is responsible for reviewing and approving or disapproving the request; however, any request for periods in excess of 120 days must be approved by the appropriate Executive Assistant Director (EAD). If approval is recommended, the completed Certification of Unavailability for Unscheduled Duty must be forwarded to Code 10A at least 30 days prior to the proposed effective date of the SA's unavailability so payment of LEAP can be suspended in a timely manner. A copy must also be provided to Code 10D (Human Capital Development). The SAC/DAD will also review and validate continuing cases of unavailability at least every 90 days.

(4) Code 10A is responsible for initiating the appropriate personnel action to suspend LEAP, and for the timely reinstatement of LEAP once a hardship has been resolved.

15-4.5. Monitoring and Managing the Substantial Hours Requirement.

a. SAs are responsible for:

(1) Monitoring their unscheduled duty hours to ensure they are complying with the substantial hours requirement.

(2) Notifying their supervisors when they perceive they may be unable to meet the substantial hours requirement.

(3) Responding when called upon to perform work during unscheduled duty hours.

b. Supervisors of SAs are responsible for:

(1) Monitoring unscheduled duty hours, and taking corrective action where necessary, to ensure the annual substantial hours requirement is consistently met.

(2) Taking corrective action as soon as it becomes evident that an SA will not be able to perform a sufficient number of unscheduled work hours to meet the substantial hours requirement.

(3) Conducting a preliminary review of the case to determine whether or not the shortfall has been caused by the SA's misconduct (e.g., refusal to work the unscheduled duty hours), or by scheduling and planning issues or deficiencies.

(4) Monitoring workload and assignments to ensure SAs under their supervision have sufficient opportunity to meet the substantial hours requirement.

(5) Carefully reviewing and validating the facts, and when appropriate, contacting Code 10A for assistance in considering an action to suspend LEAP. The suspension of LEAP is an "Adverse Action"; therefore, Code 10A's Employee Relations Specialist and the NCIS Legal office (Code 00L) must be involved in reviewing, preparing, and initiating actions that could result in the suspension of LEAP.

c. Code 10A is responsible for:

(1) Maintaining current copies of SA certifications of availability/ unavailability; and,

(2) Generating quarterly and ad hoc management reports reflecting the status of certifications of availability and the substantial hours requirement. By the 15th of February, May, August, and November of each year, Code10A, in cooperation with Code 15, will provide a report to the SACs/DADs of the unscheduled duty hours reported by each of their SAs, as well as whether or not they are meeting the substantial hours requirement. A copy of this report will also be provided to Code 10.

(3) Ensuring that all considerations for decertifying an SA's availability for unscheduled duty are coordinated with Code 00L, and that resulting actions are consistently applied across NCIS.

d. SACs/DADs are responsible for ensuring that immediate attention is given to resolving deficiencies.

15-4.6. Duration of Certifications of Availability for Unscheduled Duty. Once an SA has been certified as available for unscheduled duty, the certification remains in effect until:

a. Superseded by a subsequent annual certification; or,

b. Superseded by an SA's submission, and the appropriate supervisory approval, of a Certification of Unavailability for Unscheduled Duty. Temporary medical conditions will not affect an SA's availability for unscheduled duty unless the SA voluntarily requests to be unavailable for such duty; or,

c. Superseded by a finding that the SA has not, or is not expected to meet the substantial hours requirement. Any such findings will be carefully reviewed by the supervisor, and closely coordinated with Codes 10A and 00L before effecting decertification.

15-4.7. SA Accessibility. To ensure their accessibility, SAs are required to:

a. Maintain a mobile and/or hard line telephone at their residence, and provide the respective phone numbers to their supervisor and enter it into COMPASS, the internal NCIS employee database system; and,

b. Provide their supervisor a contact telephone number (if other than the above) when away from their residence for 24 hours, except when they are at work or on authorized leave; and,

c. Provide their supervisor advance notification and an emergency contact when they expect to travel outside the geographic area serviced by their office.

15-4.8. SAs Reporting and Recording of Unscheduled Duty Hours Worked. SAs and their supervisors must ensure that all unscheduled duty hours worked (commonly referred to as LEAP hours) are consistently and accurately recorded in SLDCADA. This information is a critical element in validating the substantial hours requirement, and provides valuable information in support of manpower and financial resources.

a. The "Type Hour Code" (THC) in SLDCADA will be coded as "O1" for all unscheduled duty hours worked, and for all SA operational travel time outside the regular working hours.

b. Unscheduled duty hours and travel time entries must also reflect the appropriate 4-digit "Operations Code". SAs in a "Duty Agent" status will report only the unscheduled duty hours worked during the assignment.

15-4.9. Decertification. NCIS may deny or cancel LEAP if an SA fails to perform unscheduled duty as assigned or reported, or is unable to perform unscheduled duty for an extended period due to physical or health reasons. Denials, cancellations, and reinstatements of LEAP must be carefully coordinated with Codes 10A and 00L.

a. The duration of any decertification for LEAP may be from one pay period to one year, depending on the circumstances and degree of the unscheduled duty hours deficit. When LEAP is denied or cancelled, the length of an SA's suspension from receipt of LEAP is an administrative determination at the discretion of NCIS management. Codes 10 and 00L will ensure decisions are consistently applied.

b. An involuntary suspension of LEAP is a reduction in pay, and therefore, requires the application of adverse action procedures, including affording the SA the appropriate notice period and appeal rights. Codes 10 and 00L will ensure the required adverse action policies and procedures are consistently applied.

15-5. OVERTIME

15-5.1. General information on overtime pay may be found at 5 CFR Chapter 551. Information specific to NCIS is provided below. The Director, NCIS, has authorized the following officials of NCIS to approve and order overtime when mission performance so requires:

a. NCIS ADs and DADs in coordination with the NCIS Comptroller (Code 14); or,

b. Field ffice SAC's; or,

c. Principal assistants to the above officials when acting on their behalf.

15-5.2. Overtime is requested, authorized, and recorded using the automated timekeeping system.

15-5.3. Information on compensatory time, or overtime for time spent in training, may be found at 5 CFR 551.423.

15-5.4. Information on compensatory time for time spent in a travel status on a non-work day may be found at CPM 2005-03.

15-5.5. Regularly Scheduled Overtime (RSO). RSO is overtime work that is scheduled, in writing, in advance of the workweek, i.e., no later than midnight Saturday night, and is scheduled to occur on successive days or after specified intervals.

a. SA personnel receiving LEAP will not be placed in a RSO status without specific approval from Deputy Director for Management and Administration (DDM&A). When unusual work requirements dictate, maximum use will be made of work schedule changes to ensure compliance with this policy. Overtime hours compensated as RSO may not also be used as qualifying hours for LEAP.

b. When approved, RSO must be recorded in SLDCACA and certified by the immediate supervisor or his or her designee.

15-5.6. Irregular Overtime (IOT). IOT differs from RSO in that the overtime is unscheduled. Except under extremely unusual circumstances, IOT must be approved before it is worked. For Fair Labor Standards Act (FLSA) exempt employees, supervisors have the authority to require the use of compensatory time in lieu of IOT when considered appropriate.

15-5.7. Adjustment of Work Schedules and Compensatory Time for Religious Observances. Information on the use of compensatory time for religious observance is found in 5 CFR 550 Subpart J. Field offices and headquarters codes are advised to keep a record of religious compensatory time earned and used. Coordination with Code 10A2 is necessary to ensure that compensatory time worked for religious holidays is credited appropriately.

15-5.8. Administratively Uncontrollable Overtime (AUO). AUO is payable to non-SA employees in positions not covered by NSPS and which require substantial amounts of irregular or unscheduled overtime work wherein the employee is responsible for independently recognizing those circumstances which require the employee to begin or remain on duty. There is no provision under NSPS for the payment of AUO.

a. A substantial amount of overtime work is defined as a minimum average of 3 hours per week. The irregular work must be a continuing requirement, generally performed more than once a week. There must be a clear anticipation that the circumstances requiring AUO will continue.

b. The responsibility for independently recognizing the requirement to remain on duty must be a definite, official, and special requirement of the position. A supervisor may restrict the duties of a position and the resultant requirement for additional hours of work in those situations deemed necessary.

c. A limited number of employees at overseas locations, whose duties and additional hours of work have been reviewed and determined to be qualifying for AUO, will receive such premium pay if authorized by NCIS Headquarters (NCISHQ).

d. Individuals newly hired to qualifying positions will receive an initial AUO rate of 15 percent effective upon their date of hire. This rate will continue until they have worked a qualifying period of time (usually one quarter). A "look-back" review will be conducted at that time and any required changes to the AUO rate effected at that time.

(1) AUO Table. AUO will be paid in accordance with the following table:

Bi-Weekly Average Hours	Premium Pay Percentage
<6 Hours	Zero (0)
6.0-10.1	Ten (10)
10.2-14.2	Fifteen (15)
14.3-18.4	Twenty (20)
18.5 and higher	Twenty-five (25)

(2) Quarterly Calculations. The continued authorization for the use of AUO and the rate at which it is paid will be reviewed on a quarterly basis to coincide with the end of the second, eight, fifteenth and twenty-first pay periods. The biweekly average of qualifying AUO hours shall determine the rate to be set for the succeeding quarter. Calculations to determine the biweekly average will exclude the following: holidays; full days of paid leave (annual, sick, military, court, and administrative); approved LWOP (excluding suspensions and absent without leave (AWOL); training (not to exceed an aggregate of 60 workdays in a calendar year); travel for administrative and Permanent Change of Station (PCS) purposes; and, periods of limited duty status. Personnel attending NCIS-directed or sponsored training may not, by federal regulations, count independent study as AUO. Compensation (pay or compensatory time-off) for irregular hours of overtime in excess of the bi-weekly averages noted above is not authorized.

(3) Employee Transfer. If an employee transfers to a new duty station in a position for which AUO is authorized, the losing office (or, NCISHQ) will forward to the gaining office (or, NCISHQ) the amount of AUO worked by the employee for that calendar year. The gaining office (or, NCISHQ) will include AUO for the new employee in its quarterly/annual reports.

(4) Pay Provisions. AUO is not considered base pay for retirement or for computing foreign or non-foreign allowances and differentials.

15-6. COMPENSATORY TIME

15-6.1 Employees covered by the FLSA may request compensatory time instead of payment for irregular or occasional overtime work. For FLSA-exempt employees, supervisors have the authority to require compensatory time in lieu of overtime when considered appropriate.

15-6.2. Compensatory time is credited hour for hour for the overtime work and is maintained in a special leave-type account for the employee's future use. There is no maximum amount of compensatory time an employee may accumulate in the payroll system.

15-6.3. The payroll system will date-age all compensatory time as it is earned. Regardless of balance totals, if any earned compensatory time remains on the books for more than one year, it will be paid out as overtime at the rate in effect when the compensatory time was actually earned.

15-6.4. Compensatory time off should be taken within a reasonable period of time after the work is performed, ordinarily within 30 days. Normally, compensatory time will be granted before annual leave is approved except when annual leave will otherwise be forfeited.

15-7. COMPENSATORY TIME OFF FOR TRAVEL (CTOFT)

15-7.1. Authority. Section 203 of Public Law 108-411 of 30 Oct 04 amended Title 5, USC, by adding section 5550b, which authorizes a new form of compensatory time off for time spent by eligible employees in a travel status away from the employee's official duty station when the travel time is not otherwise compensable. On 27 Jan 05, the Office of Personnel Management

(OPM) added interim implementing regulations through 5 CFR 550, subpart N and CPM-2005-03. Both law and regulation were effective 28 Jan 05.

15-7.2. Exclusions. Members of the Senior Executive Service are not eligible for CTOFT.

15-7.3. Special CTOFT Provisions for SAs receiving LEAP. SAs receiving LEAP may only accrue CTOFT for non-operational travel (e.g., training and conferences), and the travel must be approved in advance by their supervisor. Operational travel is covered by LEAP and will not be a basis for accruing CTOFT. Additionally, the first two hours of overtime on any day containing a part of an SA's basic 40-hour workweek are covered by LEAP, without regard to whether the hours are scheduled or unscheduled, and therefore can not be considered for the purpose of accruing CTOFT.

a. SAs may opt to claim non-operational travel time as LEAP hours in order to meet the substantial hours requirement in NCIS-1, Chapter 15, section 15-4.

b. SACs/DADs will monitor non-operational travel requirements to ensure, to the extent possible, that such travel occurs during the normal workweek, and that related decisions are being consistently applied.

15-7.4. Definitions. For the purpose of this policy:

a. Accrued compensatory time off means the CTOFT earned by an employee that has not been used or forfeited.

b. Compensable refers to periods of time that are creditable as hours of work for the purpose of determining a specific pay entitlement, even when that work time may not actually generate additional compensation because of applicable pay limitations.

c. Compensatory time off means CTOFT that is credited under this policy.

d. Official duty station means the geographic area surrounding an employee's regular work site that is the same as the area designated by NCIS for the purpose of determining whether travel time is compensable for the purpose of determining overtime pay.

e. Rate of basic pay means the rate of pay fixed by law or administrative action for the position held by an employee, including any applicable locality payment under 5 CFR part 531, subpart F; special rate supplement under 5 CFR part 530, subpart C; or, similar payment or supplement under other legal authority, before any deductions and exclusive of additional pay of any other kind.

f. Regular working hours means the days and hours of an employee's regular hours of an employee's regularly scheduled administrative workweek established under 5CFR part 610.

g. Scheduled tour of duty for leave purposes means an employee's regular hours for which they may be charged leave under CFR part 630 when absent. Section 15-2, defines the normal

workday for NCIS employees as 0730-1600. Supervisors may authorize a Compressed Work Schedule (CWS) if the mission and functions of the immediate organization permit this flexibility. SAs are not eligible for a CWS. For full-time employees, it is the 40-hour basic workweek as defined in 5 CFR 610.102. For employees with an uncommon tour of duty as defined in 5 CFR 630.210, it is the uncommon tour of duty. When an employee is on a temporary duty assignment, or otherwise absent from the permanent duty station, he or she may be required to work tours of duty that do not coincide with the tour normally worked. In such situations, it is imperative that the new tour of duty and the actual working hours are clearly communicated between the employee and the supervisor.

h. Travel means officially authorized travel (i.e., travel for work purposes that is approved by an authorized NCIS official or otherwise authorized under established NCIS policies).

i. Travel status means travel time as described in 5 CFR 550.1404 that is creditable in accruing compensatory time off for travel, excluding travel time that is otherwise compensable under other legal authority.

15-7.5. Creditable Travel Time.

a. Subject to the conditions described below, NCIS will credit an employee with compensatory time off for time in a travel status if:

(1) The employee is required to travel away from the official duty station; and,

(2) The travel time is not otherwise compensable hours of work.

15-7.6. Travel Status. Time in travel status includes the time an employee actually spends traveling between the official duty station and a TDY station, or between two TDY stations, and the usual waiting time that precedes or interrupts such travel, subject to the following guidelines, exclusions, and requirements.

a. Guidelines:

(1) Time spent at a TDY station between arrival and departure is not time in a travel status. The employee’s time in a travel status ends when he or she arrives at his or her TDY worksite or lodging site at the TDY station, wherever the employee arrives first.

(2) Time in a travel status resumes when the employee departs from the TDY worksite or lodging site at the TDY station, whichever the employee departs last.

(3) Travel time in connection with an employee's permanent change of station is not time in a travel status.

(4) Airline travelers are generally required to arrive at a designated pre-departure time (e.g., 1 or 2 hours before the scheduled departure). Such waiting time at the airport is considered usual waiting time and is creditable time in a travel status. In addition, time spent at an intervening

airport waiting for a connecting flight also is creditable time in a travel status. In all cases, determinations regarding what are creditable as "usual waiting time" are within the sole and exclusive discretion of NCIS. NCIS has defined the creditable "usual waiting period" as 2 hours.

b. Exclusions: If an employee experiences an extended (i.e., not usual) waiting time between actual periods of travel during which the employee is free to rest, sleep, or otherwise use the time for own purposes, the extended waiting time is not creditable as time in a travel status. An extended period that occurs during an employee's regular working hours is compensable as part of the employee's regularly scheduled administrative workweek.

c. Requirements.

(1) Travel between Home and a TDY Station.

(a) If an employee is required to travel directly between his or her home and a TDY station outside the limits of the employee's official duty station, the travel time is creditable as time in a travel status if otherwise qualifying. However, NCIS will deduct from such travel hours the time the employee would have spent in normal home-to-work or work-to-home commuting.

(b) In the case of an employee who is offered one mode of transportation and who is permitted to use an alternative mode of transportation, or who travels at a time or by a route other than that selected by NCIS, then NCIS will determine the estimated amount of time in a travel status the employee would have had if the employee had used the mode of transportation offered by NCIS, or traveled at the time or by the route selected by NCIS. In determining time in a travel status, NCIS will credit the employee with the lesser of the estimated time in a travel status or the actual time in a travel status.

(c) In the case of an employee who is on a multiple-day travel assignment and who chooses, for personal reasons, not to use temporary lodgings at the TDY station, but to return home at night or on a weekend, only travel from home to the TDY station on the first day and travel from the TDY station to home on the last day that is otherwise qualifying as time in a travel status under this subparagraph is mandatorily creditable (subject to the deduction of normal commuting time). Travel to and from home on other days is not creditable travel time unless NCIS, at its discretion, determines that credit should be given based on the net savings to the government from reduced lodging costs, considering the value of lost labor time attributable to CTOFT. The dollar value of an hour of CTOFT for this purpose is equal to the employee's hourly rate of basic pay as defined in 5 CFR 550.103.

(2) Time Spent Traveling To or From a Transportation Terminal as Part of Travel Away From the Official Duty Station. If an employee is required to travel between home and a transportation terminal (e.g., airport or train station) within the limits of official duty station as part of travel away from that duty station, the travel time outside regular working hours, to or from the terminal, is considered to be equivalent to commuting time and is not creditable time in a travel status. If the transportation terminal is outside the limits of the employee's official duty station, the travel time to or from the terminal, outside regular working hours, is creditable as

time in a travel status, but is subject to an offset for the time the employee would have spent in normal home-to-work or work-to-home commuting. If the employee travels between a worksite and a transportation terminal, the travel time outside regular working hours is creditable as time in a travel status, and no commuting time offset applies.

(3) Travel Involving Two or More Time Zones. When an employee's travel involves two or more time zones, the time zone from the point of first departure must be used to determine how many hours the employee actually spent in a travel status for the purpose of accruing CTOFT.

15-7.7. Crediting CTOFT.

a. Management Responsibility.

(1) SACs and DADs who have delegated authority to direct travel, and approve leave, also have the authority to credit and approve the CTOFT.

(2) The Under Secretary of Defense Memo for Secretaries of the Military Departments, of 12 Aug 05, requires that official travel be scheduled to occur during an employee's tour of duty, consistent with mission requirements. Director, NCIS has further emphasized this requirement by directing that, to the extent possible, official TDY travel should be scheduled to occur during regular working hours. Only in cases where this is not practicable will employees earn entitlement to CTOFT.

(3) NCIS will credit CTOFT in increments of one-tenth of an hour (6 minutes).

(4) CTOFT will be tracked and managed separately from other forms of compensatory time off.

(5) The supervisor is responsible for ensuring that any CTOFT earned is appropriately approved and reported in the timekeeping system.

(6) The Type Hour code for CTOFT earned is always "CB". For SAs, the SLDCADA operation code AD14 should be used. For non-SA personnel, either AD14 or the SLDCADA operation code which best describes the activity performed should be used.

b. Employee Responsibility.

(1) Requesting CTOFT. An eligible employee who performs official travel may request compensatory time off for time spent in a travel status away from the official duty station if the travel is not otherwise compensable as defined above. An employee must request credit for CTOFT by providing documentation of the time that he or she spent in an official travel status. An employee's request for credit of CTOFT may be denied if the request is not filed within the time period required by the following subparagraph.

(2) Timeliness Standard for Requesting Compensatory Time Off for Travel. An employee must submit his or her request for CTOFT within 10 workdays after returning to the official duty station or within 10 workdays of returning from TDY, or approved leave which immediately follows the TDY, during which the CTOFT was earned. The employee's request must include a detailed copy of his or her travel itinerary, and any other documentation required by the employee's supervisor. As a minimum, the request must include:

(a) Date, time, and place of departures and arrivals.

(b) Actual time spent traveling to and from transportation terminals.

(c) Time spent waiting at the transportation terminals, including arrival and departure dates and times.

(d) Time spent in actual travel, including beginning and ending dates and times.

(e) Time of arrivals and departures from temporary duty stations.

(f) Duration of normal home-to-work commuting time.

(g) Regular tour of duty days and hours.

15-7.8. Use of Accrued Compensatory Time Off.

a. Employees must request permission from their supervisor to schedule the use of accrued CTOFT.

b. CTOFT may be used when the employee is granted time off from scheduled tour of duty. An employee may use earned CTOFT in increments of one-tenth of an hour (6 minutes).

c. NCIS will charge CTOFT in the chronological order in which it was earned, with the CTOFT earned first being charged first.

d. The Type Hour code for CTOFT used is "CF". The operational code is "TTLV".

15-7.9. Forfeiture of Unused CTOFT.

a. An employee shall forfeit claim to CTOFT if the claim is not submitted within the time limits described above.

b. An employee must use accrued CTOFT by the end of the 26th pay period after the pay period during which it was credited. If an employee fails to use the CTOFT within 26 pay periods after it was credited, he or she will forfeit the CTOFT. The only exception to this requirement is where the employee's failure to use his or her CTOFT earned was due to an exigency of the service beyond the employee's control. In those cases, the DAD for Human

Resources Operations and Services, Code 10A, at his or her sole and exclusive discretion, may extend the time limit for using such CTOFT up to an additional 26 pay periods.

c. When an employee with unused CTOFT separates from federal service, or is placed in a leave without pay status in the following circumstances, and later returns to service with the same (or, successor) agency, he or she must use all accrued CTOFT by the end of the 26th pay period following the pay period in which he/she return to duty, or the CTOFT will be forfeited.

(1) Performing Service in the Uniformed Services. The employee separates or is placed in a LWOP to "perform service in the uniformed services" and later returns to service through the exercise of a reemployment right provided by law, Executive Order, or regulation.

(2) Separation or LWOP. The employee separates or is placed in a LWOP status because of an on-the-job injury with entitlement to injury compensation under 5 USC Chapter 81 and later recovers sufficiently to return to work.

d. When an employee voluntarily transfers to another agency (including a promotion or change to lower grade action), he or she must forfeit unused CTOFT.

e. Upon Separation. When an employee separates from federal service, any unused CTOFT is forfeited.

f. Upon Movement to a Non-Covered Position. When an employee moves to a federal position not covered by this policy, he or she forfeits any unused CTOFT. This requirement does not prevent the successor agency from using another legal authority to give the employee credit for CTOFT equal to the forfeited amount.

15-7.10. Prohibition Against Payment for Unused CTOFT. There is no limit to the amount of CTOFT an individual may earn; however, an individual may not receive payment under any circumstances for any unused CTOFT earned under this policy. This prohibition against payment also applies to surviving beneficiaries in the event of the individual's death.

15-7.11. Inapplicability of Premium Pay and Aggregate Pay Caps. Accrued CTOFT under this policy is not considered in applying the premium pay limitations established under 5 USC 5547 and 5 CFR 550.105 through 5 CFR 107 or the aggregate limitation on pay established under 5 USC 5307 and 5 CFR part 530, subpart B.

15-8. RECRUITMENT, RETENTION AND RELOCATION INCENTIVES

15-8.1. NCIS fully complies with the regulations governing recruitment, retention and relocation incentives found at 5 CFR 575.

15-8.2. Decisions to authorize one or more of these incentives to particular categories of employees will be announced via an NCIS Gen Admin.

15-9. LEAVE

15-9.1. General information on leave may be found at 5 CFR 630. This reference includes information on all authorized types of leave including annual leave, sick leave, holiday leave, LWOP, and family medical leave. Information specific to NCIS is provided in the following sections.

a. Leave will be requested, approved, and recorded using the automated timekeeping system.

b. Leave may be taken in six-minute increments. The amount of leave charged for a full-day's absence depends on the normal work schedule for that day, e.g., 8 hours, 9 hours or 10 hours.

15-10. HOME LEAVE

15-10.1. Information on eligibility for and applicable rates for home leave may be found at 5 CFR 630 Subpart F.

15-10.2. As authorized by this subpart and Title 5 USC section 6305(a), NCIS employees assigned to duty stations abroad may be eligible for home leave if the following conditions apply:

a. An employee serving at a post for which payment of a foreign or non-foreign differential of 20 percent, or more, is authorized, may receive 15 days of home leave for each 12 months of service abroad.

b. An employee serving at a post for which payment of a differential of at least 10 percent but less than 20 percent is authorized 10 days of home leave for each 12 months of covered service.

15-10.3. More specific information on computation of home leave entitlements may be found in the above references.

15-11. EXCUSED ABSENCE

15-11.1. Excused absence refers to an authorized absence from duty without loss of pay and without charge to other types of leave. Information on the use of excused absence may be found at the DoD Civilian Personnel Manual Chapter 630.

a. The Director, NCIS, has delegated authority to approve excused absences under this authority to DAD and SAC personnel. In very limited circumstances, these officials may authorize excused absences of up to 59 minutes at the beginning or end of a workday. Excused absences in excess of 59 minutes may not be used to create or extend a holiday.

b. Adverse Weather Conditions. For offices in the Washington, DC metro area, NCIS will follow the direction of the OPM with regards to dismissals or cancellation of work due to inclement weather conditions. Information on the status of government options may be found at

the OPM website. Outside the Washington, DC metro area, NCIS offices will follow the guidance of the local Navy or Marine Corps commander or an alternative government entity.

c. Late Arrival. For employees in the Washington, DC metro area, OPM may announce that a delayed arrival policy is in effect. Normally, this will allow covered employees to arrive at work up to 2 hours later than their normal arrival time. Non-emergency employees who arrive late but within the authorized timeframe will be excused without loss of pay or charge to leave. For areas outside the Washington, DC metro area, local authorities may announce that a late arrival policy is in effect for federal workers. This means that a reasonable period of time, up to 2 hours, will be allowed for employees to report for duty without charge to leave.

15-12. VOLUNTARY LEAVE TRANSFER PROGRAM

15-12.1. General information on the Voluntary Leave Transfer Program may be found at 5 CFR 630 Subpart I. Information specific to NCIS is provided below.

a. Procedures for Leave Recipients

(1) A leave recipient application (OPM Optional Form 630) should be submitted to the DAD for Personnel Operations and Services, Code 10A, who will approve/disapprove all leave recipient applications.

(2) Prior to submission, the potential leave recipient's supervisor will determine if the absence from duty without available paid leave because of the medical emergency is (or, is expected to be) at least 24 hours. The hours of absence from duty without available paid leave need not be consecutive, but must have resulted from the same medical emergency for which the employee made an application for a leave transfer.

(3) Leave recipients will be notified in writing within 10 days of the approval/disapproval of their request. If the leave recipient's request is disapproved, the employee shall be notified of the reason for disapproval and grievance rights under the DON administrative grievance procedure. If the potential leave recipient's application is approved, Code 10A will notify the recipient, in writing within 10 days, of the following: the leave recipient's responsibility to provide documentation to support the continuation of the medical emergency; the conditions under which the medical emergency terminates; and, the specific procedures the leave recipient will be required to follow to notify Code 10A of the termination of the medical emergency.

b. Procedures for Leave Donors.

(1) To become a leave donor, a Request to Donate Leave to a Leave Recipient (within DON) (Optional Form 630A) or Request to Donate Leave to Leave Recipient (outside DON) (Optional Form 630B) will be completed. Potential donors must add their servicing payroll office number and the name of the recipient's employing activity in the appropriate blocks.

(2) If the leave donor's application is approved, the donor shall be notified in writing of: the limitations on donation of annual leave; the number of hours of his or her annual leave which

will be transferred; and the employee's entitlement to have a portion of the unused transferred annual leave restored to his or her annual leave account (in increments of one hour) at the termination of the leave recipient's medical emergency. In any one year, a leave donor may donate no more than a total of one-half of the amount of annual leave he or she would be entitled to accrue during the leave year in which the donation is made. Leave donors who are projected to have annual leave that would be subject to forfeiture at the end of the leave year may donate, at a maximum, the lesser of: ,one-half of the amount of annual leave he or she would be entitled to accrue during the leave year in which the donation is made, or the number of hours remaining in the leave year (as of the date of the transfer) for which the donor is scheduled to work and receive pay.

(3) The DAD for Personnel Operations and Services, Code 10A, may approve waivers of the limitations on annual leave donations. Requests for waivers shall be submitted in a separate written statement signed by the donor certifying that the donor is aware that the request exceeds the limitations and describing the unusual circumstances inherent in the request. The approved waiver request should be forwarded with the donor's application to Code 10A2. Code 10A will accept donations of annual leave from donors employed by other agencies when either a family member of a leave recipient is employed by another agency and requests the transfer of annual leave, or the amount of annual leave transferred from leave donors employed by the leave recipient's employing agency may not be sufficient to meet the needs of the leave recipient. Annual leave shall be transferred in increments of one hour.

c. Retroactive Adjustments. Transferred annual leave may be substituted retroactively for periods of LWOP used to liquidate the indebtedness for advanced annual or sick leave, granted on or after the date designated by Code 10A, as the beginning of the medical emergency.

d. Records. Code 10A2 must maintain the following records for OPM inspection: the number of applications approved for medical emergencies affecting the employee and the number of applications approved for medical emergencies affecting an employee's family member; the grade or pay level of each leave recipient and leave donor; the total amount of leave transferred to each leave recipient's annual leave account; the estimated cost related to administering the voluntary leave transfer program; the gender of each leave recipient; the number of leave recipients who returned to work after the termination of the medical emergency; and, the number of leave recipients who retire on disability retirement under Civilian Service Retirement System (CSRS) or Federal Employee Retirement System (FERS) regulations within 6 months after the termination of the medical emergency.

e. Tax Information. Employees are to be aware that Internal Revenue Service (IRS) has determined that the income received from the use of donated annual leave is taxable to the leave recipient. The IRS has also ruled that a leave donor does not incur a deductible expense or loss upon the use by a leave recipient.

15-13. TELEWORK

15-13.1. The NCIS telework program allows selected employees to perform work at sites other than the traditional office. Telework may be used to resolve a number of work/life issues,

including accommodation of special needs or disabilities, energy or environmental conservation, cost or space savings, or better geographic coverage for the NCIS mission. While telework is not intended to be a substitute for family care, it may enhance the quality of family life through savings in commuting time. The telework program is not an entitlement, but rather, an optional work arrangement which may be mutually beneficial to the employee and NCIS.

15-13.2. Employees eligible for telework occupy positions involving tasks and work activities that are portable, do not depend on regular face-to-face interaction with other agency employees or customers, and which are conducive to electronic communication or oversight by the supervisor. Tasks and functions generally suited for telework include thinking and writing; policy development; research; analysis (e.g., investigating, program analysis, policy analysis, financial analysis); report writing; telephone-intensive tasks; computer-oriented tasks (e.g., programming, data entry, word processing, web page design); or, data processing.

15-13.3. Employees not generally eligible for telework occupy positions involving tasks that require the employee to have daily face-to-face contact with the supervisor, colleagues, clients, or the general public, which cannot otherwise be achieved via email, telephone, fax or similar electronic means; require access to classified information; and/or, are at the trainee or entry level. Positions shall not be automatically excluded on the basis of occupation, series, grade or supervisory status. No classified documents (hard copy or electronic) may be taken to an employee's home. Any work that requires the use of such documents is ineligible for telework.

15-13.4. Certain demonstrated personal characteristics are considered best suited to telework arrangements. These include dependability, ability to handle responsibility independently, a proven record of high personal motivation, ability to prioritize work effectively and utilize good time management skills, and a consistent record of "Level 3 – Valued Performer", or equivalent, performance ratings. Employees who have not completed the trial or probationary period are generally not eligible for telework arrangements as this period is established to allow supervisors an opportunity to personally observe and evaluate their performance.

15-13.5. There are two types of telework: "regular and recurring" and "ad hoc".

a. Regular and recurring telework means an approved work schedule that includes at least one day per pay period working from an alternative worksite. This arrangement is ideal for employee's whose work regularly involves independent activities described in subparagraph 15-13c above and who have demonstrated the characteristics outlined in subparagraph 15-13.e.

b. Ad hoc telework is occasional or irregular work by an employee at an alternative worksite. This arrangement is ideal for employees who infrequently are required to complete a specific project or report, conduct research, or prepare an instruction or directive.

15-13.6. The following general rules apply to telework participation by NCIS employees:

a. The employee's official duty station, as noted on the Notification of Personnel Action (SF-50), is used to determine locality pay adjustments, special salary rates, travel entitlements, etc.

b. Existing rules regarding hours of work apply. The supervisor, with employee participation, will determine the employee's work schedule consistent with operational requirements. At the supervisor's discretion, an employee who participates in telework may work a Compressed Work Schedule.

c. Existing rules regarding pay, leave, overtime and timekeeping apply.

d. Position descriptions and performance appraisals do not require revision due to the employee's participation in telework.

e. Employees who telework, are covered by the Federal Employees' Compensation Act (FECA) in the event of an on-the-job injury or occupational illness. The employee must notify the supervisor immediately of any accident or injury that occurs while working at home.

f. Telework shall not be used as a substitute for dependent (child, elder, spouse, etc.) care. Employees should not be caring for dependents when they are working at home.

15-13.7. Teleworkers are responsible for the security of all official information and the protection of any government furnished equipment and property. Employees may bear legal, pecuniary or criminal responsibility, depending on the circumstances, if government equipment is misused, lost, damaged or stolen. Misuse includes use of government equipment for personal business. Additionally, there are stringent penalties for the willful and unlawful destruction, damage, unauthorized removal, or alienation of federal records.

15-13.8. NCIS assumes no responsibility for any operating costs associated with an employee using his/her personal equipment and residence while teleworking. This includes home maintenance, insurance and utilities. NCIS will, however, provide the employee all necessary office supplies required for telework.

15-13.9. Participation in the telework program may be initiated by the employee or the supervisor. Final determination of which positions and employees are suitable for telework will be at the discretion of the SAC, DAD, or equivalent supervisor, and based on the:

a. Suitability of the work to be performed.

b. Career status and work performance history of the employee.

c. Availability of necessary computer equipment.

d. Compliance of the proposed work site with security and Privacy Act requirements.

15-13.10. SACs, DADs, or equivalent supervisors, may approve ad hoc telework arrangements where the employee's work regularly involves independent activities described in subparagraph 15-13.c above and where the employee has demonstrated the characteristics outlined in subparagraph 15-13.e. Regular and recurring telework arrangements must be forwarded to Code 10A for approval prior to execution. Telework arrangements involving a change to the

employee's regular duty station must be approved by the DDM&A. In all cases, a telework agreement, available from Code 10A, must be executed between the employee and the first-line supervisor prior to initiation of telework. The supervisor will maintain a record of those employees authorized to telework on a regular and recurring basis, and the frequency of the telework. Also to be retained is the identification of any employee who is not authorized to participate in telework and the specific reason given to the employee for disapproving his or her request to participate in the program. Telework participation will be terminated if an employee's performance does not meet the prescribed standard or if the telework arrangement fails to meet mission requirements.

15-13.11. Employees who are not approved for telework participation, or whose telework participation is terminated, may appeal this decision through the chain of command to their respective AD or EAD.

APPENDIX (1): CERTIFICATION OF "AVAILABILITY" FOR UNSCHEDULED DUTY

Law Enforcement Availability Pay (LEAP): Special Agents (SAs) are paid LEAP if their annual average of unscheduled duty hours worked, divided by the total number of regular workdays for the same period, is equal to or greater than 2 hours – referred to as the "Substantial Hours Requirement".

Certification Requirement: SAs and their supervisors must "certify" an SA's availability for unscheduled duty hours by completing and submitting this document as follows:

1. New SAs: New SAs and their supervisors must certify that the SAs are expected to meet the Substantial Hours Requirement during the upcoming 1-year period.

2. Annual Certification: All SAs receiving LEAP, and their supervisors, must annually certify (by 15 January) that the SAs currently meet, and are expected to continue to meet the Substantial Hours Requirement during the upcoming 1-year period.

3. Filing Requirements: Completed and signed certification documents must be forwarded to Code 10A12 (Pay and Entitlements Branch) as follows:

   a. New SAs: Within 2-weeks of their entry on duty date.

   b. Annual Certifications: By 30 January.

Certification: I, _____, certify that I expect to be able to perform official duties during unscheduled duty hours and agree to be available for unscheduled duty based on the needs of the Naval Criminal Investigative Service (NCIS). To ensure my availability, I certify that I understand and agree to the following conditions:

1. I will maintain a mobile and/or hard line telephone at my residence, and will provide the phone number(s) -- whether listed, unlisted, or unpublished -- to my supervisor.

2. I will provide my supervisor a contact telephone number (if other than the above) when I will be away from my residence for 24 hours, except when I am at work or on authorized leave (sick, annual, administrative, relocation, or leave without pay).

3. I will provide my supervisor advance notification, and an emergency contact telephone number, when I expect to travel outside the geographic area serviced by my office.

4. I will not engage in any employment other than my work as a NCIS Special Agent unless I have specific and current authorization from NCIS Headquarters allowing me to do so.

I understand this "Certification of Availability for Unscheduled Duty" remains in effect until superseded by the next annual certification, by a written notice from me to my supervisor

advising that I am no longer available for unscheduled duty, or as the result of a finding by my supervisor that I have not, or am not expected to meet the Substantial Hours Requirement.

I also understand I am responsible for consistently and accurately recording all unscheduled duty hours worked (commonly referred to as LEAP hours) in SLDCADA.

_____	_____
SA's Signature	Date Signed
_____	_____
Supervisor's Signature	Date Signed

SAs and their supervisors will closely monitor unscheduled duty hours, and take corrective action when necessary to ensure the annual Substantial Hours Requirement is consistently met.

APPENDIX (2): CERTIFICATION OF "UNAVAILABILITY" FOR UNSCHEDULED DUTY

Law Enforcement Availability Pay (LEAP): Special Agents (SAs) are paid LEAP if their annual average of unscheduled duty hours worked, divided by the total number of regular workdays for the same period, is equal to or greater than 2 hours – referred to as the "Substantial Hours Requirement". NCIS may deny or cancel LEAP if an SA fails to perform unscheduled duty for an extended period due to physical or health reasons.

Request for Unavailability: I, _____, request that I be assigned no overtime work, or unscheduled duty hours, beginning on _____. I intend to be available again for overtime work and unscheduled duty hours on _____.

Reason for Unavailability: I make this request because of the following described personal or family hardship:

Statement of Understanding: I understand that if my request is approved, LEAP will not be payable during the period I have designated above, or for any extensions of this period that I request and that are subsequently approved by proper authority. I also understand and acknowledge that the non-payment of LEAP that results from my request is not an adverse action taken by management.

Certification: I hereby certify that the above request is based upon my own personal or family hardship and is made voluntarily:

_____
Signature of Requesting Special Agent

_____
Date of Request

☐ Approved ☐ Disapproved

_____ _____
Signature of DAD or SAC Date

Filing Requirement: If unavailability is approved, a copy of this completed and signed document must be forwarded to Code 10A12 (Pay and Entitlements Branch) at least 30 days prior to the approval date of the suspension of availability so the payment of LEAP can be suspended in a timely manner.

APPENDIX (3):

157795 13:31 20110902 IN:SSDEMAIL #38299 OUT:NCISWWSSD #50

GENERAL ADMINISTRATION 02SEP11

FROM: 0000 GEN: 11-0031

TO: DIST

SUBJ: NCIS POLICY DOCUMENT 11-17: ADMINISTRATIVE (HOURS OF WORK)

REFERENCE
(A) NCIS-1, Chapter 15

1. Section 15-2.2.a of reference (a) is superseded by the following:

2.2.a. The normal workday is 0730-1600, which includes a 30-minute unpaid lunch break. A longer break of up to 60 minutes can be accommodated, at the supervisor's discretion, as long as the work schedule is extended by the same amount so as to retain the 8 hour workday. Lunch breaks may not be scheduled at the beginning or end of the workday for the purpose of providing for late arrival or early departure except in highly unusual circumstances when, for example, an employee is required to work through the lunch period because of a critical requirement occurring on that work day. Employees may, with the approval of their supervisor, set work schedules that vary by up to 90 minutes before or after the normal starting time of 0730. Work schedules should remain constant.

2. Section 15-2.2.b.(5) of reference (a) is superseded by the following:

2.2.b.(5). Any day of the workweek, Monday through Friday, may be used as the "off" day in a CWS schedule. Likewise, any day of the workweek may be used as the short (8-1/2 hour) workday. However, the established non-workday and the short day will remain constant each pay period unless operational requirements dictate that the day(s) be changed. Tours of duty under the CWS must fall within the normal scheduling times and therefore must not begin earlier than 0600 or end after 1800, and must include a minimum 30-minute lunch break, with the requisite extension of the workday to accommodate breaks of longer than 30 minutes.

3. This policy will be incorporated in the next revision of NCIS-1, Chapter 15.

4. The point of contact for this document is (b)(6) Management Assistant for Code 10, Human Resources Operations and Services. She can be reached at (b)(6) or (b)(6) @navy.mil.

FOR OFFICIAL USE ONLY
PAGE 1 LAST (b)(6)

APPENDIX 4

815495 10:25 20140127 IN:SSDEMAIL #109446 OUT:NCISWWSSD #1564

GENERAL ADMINISTRATION 27JAN14

FROM: 0000 GEN: 11C-0006

TO: DIST

SUBJ: POLICY DOCUMENT 14-01: ADMINISTRATIVE (LAW ENFORCEMENT AVAILABILITY PAY - LEAP)

REFERENCES
(A) GEN: 11C-0011 04JUN09/SUBJ: NCIS POLICY DOCUMENT 09-04: PERSONNEL (LAW ENFORCEMENT AVAILABILITY PAY (LEAP))
(B) NCIS-1, Chapter 15, Hours of Work, Pay and Leave/Mar09
(C) 5 CFR 550.181-187

1. This policy Gen Admin cancels reference (A) and updates paragraph 15-4 of reference (B), which sets forth the NCIS policy for calculating Law Enforcement Availability Pay (LEAP) hours for the Substantial Hours Requirement of reference (C) for NCIS special agents (SAs).

2. In response to a finding by the Naval Audit Service, NCIS is revising its Law Enforcement Availability Pay (LEAP) policy regarding the calculation used to determine whether or not personnel meet the Substantial Hours Requirement of reference (C). Specifically, the Naval Audit Service determined that NCIS' policy needs to include a distinction between "unscheduled hours worked on a Regular Workday" and "unscheduled hours worked on a non-Regular Workday" for the purpose of calculating LEAP hours to ensure compliance with section 550.183 of reference (C). The Naval Audit Service noted that while section 550.183 of reference (c) authorizes credit for non-duty hours in which the individual is "available to work" on a Regular Workday, it does not authorize such credit for non-regular workdays. Therefore, beginning 01Jan14 (CY-14), NCIS will apply 1 hour of LEAP for every 3 hours of LEAP worked on regular workdays as a credit for periods of availability. LEAP hours worked on!
non-regular workdays will no longer be included in calculating the 1 for 3 hour availability credit.

3. Section 15-4.1 of reference (B) is revised to read as follows:
"Purpose of LEAP. The purpose of LEAP is to provide a special premium pay to SAs to ensure their availability for unscheduled duty in excess of a 40-hour work

week, based on the needs of the employing agency. SAs receive LEAP under the provisions of Title 5 USC 5545a and 5 CFR 550.181 through 550.187."

4. Section 15-4.1.d. of reference (B) is revised to read as follows:
"SAs participating in the part time agent program (PTAP) are ineligible for LEAP for the duration of their participation in the PTAP. When submitting PTAP request, SAs must also submit a formal LEAP Opt-Out request as part of their request for PTAP."

5. Section 15-4.3 of reference (B) is changed to read as follows:

27JAN14

SUBJ: POLICY DOCUMENT 14-01: ADMINISTRATIVE (LAW ENFORCEMENT AVAILAB

"Substantial Hours Requirement. SAs are paid LEAP if their annual average of unscheduled duty hours worked in excess of the Regular Workday plus the hours credited as being available for work, is equal to or greater than 2 hours per Regular Workday. This is called the "Substantial Hours Requirement".

a. Regular Workdays. Unscheduled duty hours worked on regular workdays are counted towards the Substantial Hours Requirement at the rate of 1 hour of LEAP for every hour actually worked. SAs will also receive an additional availability credit of 1 hour for every 3 hours of LEAP actually worked. The adjusted total is calculated by dividing the actual unscheduled duty hours worked on a regular work day by 3 and multiplying the result by 4 to obtain the total unscheduled duty hours worked on regular workdays.

b. Non-regular workdays. Unscheduled duty hours worked on non-regular workdays are counted towards the Substantial Hours Requirement calculation at the rate of 1 hour of LEAP for every 1 hour actually worked on a non-Regular Workday; however, these hours are not subject to the 1 for 3 availability credit described in paragraph a.

c. For purposes of availability pay, unscheduled duty hours are those hours during which a criminal investigator performs work, or is determined by the employing agency to be available for work, that are not (1) Part of the 40-hour basic work week of the investigator; or (2) Regularly scheduled overtime (RSO) hours compensated under 5 USC 5542 and 5 CFR 550.111.

d. RSO and LEAP. For criminal investigators receiving availability pay, RSO hours compensated under 5 USC 5542 and 5 CFR 550.111 are those overtime hours

scheduled in advance of the investigator's administrative workweek, excluding the first 2 hours of overtime work on any day containing a part of the investigator's basic 40-hour workweek, as required by 5 CFR 550.111(f)(1). See section 15-5.3 for additional information on requesting RSO.

e. Calculation of the Substantial Hours Requirement. The total number of unscheduled hours is the sum of unscheduled duty hours worked on regular workdays (based on the 1 for 3 credit formula) and the actual unscheduled duty hours worked on non-regular workdays. For unscheduled hours worked on regular workdays, the Substantial Hours Requirement is calculated by dividing the unscheduled duty hours worked on a regular work day by 3 and multiplying the result by 4 to obtain the "Total Unscheduled Regular Workday Duty Hours Worked or Available for Work". This number is added to the number of actual unscheduled duty hours worked on a non-Regular Workday and the total becomes the numerator in the final calculation. This number is then divided by the "Total regular workdays" (the denominator). To meet the Substantial Hours Requirement, the resulting quotient must be equal to or greater than 2," to ensure compliance with Title 5 Code

27JAN14

SUBJ: POLICY DOCUMENT 14-01: ADMINISTRATIVE (LAW ENFORCEMENT AVAILAB

of Federal Regulations 550.183.

(1) Example 1: During the calendar year, SA #1 worked 250 Production Days (i.e. regular workdays). Over the course of these 250 Production Days, SA #1 worked 300 unscheduled duty (i.e. LEAP) hours on regular work days. In addition to these hours, SA #1 worked an additional 100 hours of unscheduled duty hours on non-regular workdays (e.g. weekends, or any day in which the SA works more than 4 hours of training, travel or leave). Based on the above scenario, the SA #1's Substantial Hours Requirement is calculated in the following manner: For LEAP Hours on regular workdays: 300/3 = 100; 100 x 4 = 400. The 400 hours are added to the hours worked on non-regular workdays, 400 + 100 = 500; which represents the total LEAP hours worked. 500 is divided by 250 (the number of Production Days), 500 divided by 250 workdays = 2 hours.

(2) Example 2: During the calendar year, SA #2 worked 225 Production Days (i.e. regular workdays). Over the course of these 225 Production Days, SA #1 worked 350 unscheduled duty (i.e. LEAP) hours on regular work days. In addition to these hours, SA #3 worked an additional 50 hours of unscheduled duty hours on non-regular workdays (e.g. weekends, or any day in which the SA works more than 4 hours of training, travel or leave). Based on the above scenario, the SA #2's

Substantial Hours Requirement is calculated in the following manner: For LEAP Hours on regular workdays: 350/3 = 116.66; 116.66 x 4 = 466.64. The 466.64 hours are added to the hours worked on non-regular workdays, 466.64 + 50 = 516.64; which represents the total LEAP hours worked. 516.64 is divided by 225 (the number of Production Days), 500/225 = 2.30 hours.

(3) Example 3: During the calendar year, SA #3 worked 225 Production Days (i.e. regular workdays). Over the course of these 225 Production Days, SA #1 worked 250 unscheduled duty (i.e. LEAP) hours on regular work days. In addition to these hours, SA #3 worked an additional 150 hours of unscheduled duty hours on non-regular workdays (e.g. weekends, or any day in which the SA works more than 4 hours of training, travel or leave). Based on the above scenario, the SA #3's Substantial Hours Requirement is calculated in the following manner: For LEAP Hours on regular workdays: 250/3 = 83.33; 83.33 x 4 = 333.33. The 333.33 hours are added to the hours worked on non-regular workdays, 333.33 + 150 = 483.33; which represents the total LEAP hours worked. 483.33/225 = 2.15 hours.

6. Section 15-4.5.c of reference (B) is changed to read as follows:
"c. Code 10A is responsible for:
(1) Maintaining records (either electronic or hard copy) of SA certifications of availability/unavailability; and, (2) Provide a final annual report no later than February 1st to the Assistant Director for Human Resources (Code 10) which lists all SAs who failed to meet the Substantial Hours Requirement. (3) Provide management reports on an as-needed basis to AD Code 10 regarding the status of certifications of availability to ensure compliance with 5 CFR 550.184.

27JAN14

SUBJ: POLICY DOCUMENT 14-01: ADMINISTRATIVE (LAW ENFORCEMENT AVAILAB

7. This change to the LEAP policy will be incorporated into the next revision to NCIS-1, Chapter 15. The POC for this policy document is the Human Resources Directorate, Personnel Operations and Services Department (Code 10A).

DISTRIBUTION
NCISHQ: All Directorates and Departments
INFO: WWSSD

FOR OFFICIAL USE ONLY
PAGE 4 LAST (b)(6)

CHAPTER 16
TITLE: NCIS EEO PROGRAM MANAGEMENT AND RESPONSIBILITIES
POC: CODE 10A
DATE: DEC 06

16-1. GENERAL

a. Purpose. This chapter affirms the commitment of the Director of the Naval Criminal Investigative Service (NCIS) to the principles of Equal Employment Opportunity (EEO), establishes policy, and assigns responsibility for the EEO Program in NCIS. In keeping with the commitment of the Secretary of the Navy, NCIS promotes equal employment opportunity for all persons in the workplace and provide maximum opportunities at all levels of the organization.

b. Scope. This chapter applies to civilian and military personnel NCIS wide.

c. Background. The following legislation and instructions provide broad guidance for implementing EEO programs within the Federal Government with regard to race, color, religion, sex, national origin, age, disability, or reprisal:

(1) Public Law 92-261, EEO Act of 1972.

(2) Rehabilitation Act of 1973, Section 501.

(3) Age Discrimination in Employment Act of 1967.

(4) DON Civilian Human Resource Manual Subchapter 1601, EEO Program Policy.

(5) Civil Rights Act of 1991 as amended.

(6) Notification of Federal Employees Anti-discrimination and Retaliation Act of 2003.

The Code of Federal Regulation (Code 29 C.F.R. 1614) and the Equal Employment Opportunity

Commission (EEOC) Management (Directive 110) establish regulations for processing complaints of discrimination within the Federal Government, and Office of Personnel Management (OPM) Instruction amplifies this guidance as Department of Navy (DON) policy.

16-2. POLICY

a. The Director of NCIS is firmly committed to support the Navy's EEO Program to ensure fair treatment and equal opportunity for both employees and applicants. Discrimination and harassment within the work environment are against policy and in direct opposition to legal mandates. This includes policy to ensure equal opportunity for advancement, to ensure every individual's maximum potential, and ensure fair and impartial review of complaints of discrimination. It also includes a workforce free from harassment sexual or otherwise by supervisors, colleagues, subordinates (civilian or military) or others who have business at NCIS. For the NCIS Equal Employment Opportunity Policy see Appendix 1, and for the NCIS Sexual Harassment Policy see Appendix 2.

b. Managers and supervisors (civilian and military) at all levels are responsible for exercising personal leadership in executing the NCIS EEO policy and achieving its objectives. No less than their full cooperation and active support in this Command endeavor is expected. Their performance in this area will be a factor included in the applicable performance evaluation system.

c. Complainants, their representatives or witnesses, EEO counselors, and EEO program officials shall be free from restraint, interference, coercion, discrimination, or reprisal at any stage during the presentation and processing of a discrimination complaint, or any time thereafter. Furthermore, this adverse behavior promotes inefficiency, wastes and inhibits productivity, and will not be condoned.

d. Affirmative employment efforts and progress towards elimination of under-representation will be directed to the plan developed that identifies deficiencies and result-oriented actions for correction. Agency-wide participation, positive support, and direct involvement of civilian and military personnel must continue to the fullest, until discrimination in any facet of employment has been eliminated.

e. Action. The NCIS EEO Program Policy Statement, Prevention of Sexual Harassment Policy, and the revised EEO Complaint Process procedures will be posted on all bulletin boards at the NCIS Headquarters, in each Field Office (FO), Resident Agency, and Resident Unit. Executive Assistant Directors (EADs), Assistant Directors (ADs), Deputy Assistant Directors (DADs), Special Agents in Charge (SACs), Assistant Special Agents in Charge (ASACs), division chiefs, branch heads, managers and supervisors will be guided by this chapter in the performance of their respective EEO duties.

16-3. DELINEATION OF EEO PROGRAM RESPONSIBILITY AND STRUCTURE

a. The EEO Officer (EEOO) is the Director of NCIS, who is responsible for a program that is effective, result- oriented, and in compliance with applicable EEO laws, regulations, DON

instructions, this chapter, and other NCIS instructions.

b. NCIS Deputy EEO Officer (DEEOO) is the principal staff advisor to the EEOO and managers at all levels, on EEO program matters. The DEEOO is responsible for establishing priorities in EEO program areas within the Command's mission and boundaries of resources. The DEEOO will provide direction and policy guidance for EEO program development, implementation and evaluation. Specific program responsibilities are:

(1) Review agency policies, procedures, actions, achievements, and barriers concerning affirmative employment efforts for women and other minority groups. This includes review of Requests for Personnel Action (SF-52), review of merit promotion panel composition and promotion certificates, and review of files before referral to the selecting official. The DEEOO will develop the Affirmative Employment Program (AEP) and recommend changes based on consultation or input from staff officials and regional managers.

(2) Manage the discrimination complaint process by taking action to expedite the complaint process and/or resolution. Conduct a continuing program to eradicate every form of discrimination from work policies and conditions that include recommending disciplinary action against personnel engaged in discriminatory practices. Provide counseling services for employees or applicants who believe they have been discriminated against because of race, color, religion, sex, national origin, age (defined as persons aged 40 years or more), disability, or reprisal.

(3) Participate with managers in the development and review of present and proposed agency policy, or decisions that affect the civilian workforce. This includes, serving on temporary or permanent committees, such as position management, job restructuring, training, publicity, or recruitment.

(4) Review, evaluate and coordinate the EEO objective of managers and supervisors in the Performance Appraisal Review System (PARS) ensuring continuing compliance of EEO policy annually. Provide orientation, training, and advice to managers and supervisors assuring understanding and implementation of the EEO policy and program.

(5) Select collateral duty EEO Counselors. Provide training and guidance to these individuals in accomplishing their assigned responsibilities.

(6) Special Emphasis Programs.

(a) Act as principal staff advisor to the EEOO, managers and supervisors on all EEO issues relating to, or impacting the status and treatment of women and other minorities. Key duties are to integrate recommendations and strategies into the agency's EEO goals and objectives by conducting studies and analyses on inclusion in recruitment, training, promotions, boards, committees, and other areas that have an influence on career progression.

(b) Serve as the principal staff advisor to the EEOO, managers and supervisors on all issues relating to, or impacting on the status and treatment of disabled individuals

or applicants. Key duties focus on identifying and presenting workable solutions to the broad spectrum of employment-related needs of disabled individuals and veterans. This encompasses the development of policies and procedures to review the attitudinal, architectural, and agency barriers to adequate and successful recruitment, hiring, placement, promotion, and ensuring a reasonable accommodation in the workplace, including accessibility.

(c) Advises the EEOO on improvement of career opportunities for lower level, underutilized employees towards upward mobility. Assists in developing an upward mobility plan for the agency. Conducts skill surveys and analyzes data to determine the most effective application of training, job restructuring, and identification of target series. Provides counseling to prospective program applicants, and orientation to program entrants. Provides information and advice to supervisors on the advantages of the upward mobility program.

(7) Create a system to annually evaluating the effectiveness of the activity's overall EEO effort. Ensure EEO reporting requirements are met.

(a) EADs, ADs, DADs, SACs , ASACs, division chiefs, branch heads, managers and supervisors are personally responsible for promoting and executing DON and NCIS EEO policies. This includes responsibility for the training of appointed EEO counselors.

(b) All managers and supervisors (civilian or military) will support the principles of EEO as an inherent part of their assigned responsibilities. They are responsible for the execution of the NCIS EEO policy and achieving its objectives. Further, they will conduct a continuing program to eradicate every form of discrimination from work policies and conditions including disciplinary action against personnel who engage in such discriminating practices. Finally, they are expected to exercise personal leadership in the establishment of local AEP activities for underrepresented or underutilized employees.

(c) EEO counselors are responsible for establishing and maintaining an open and sympathetic channel through which employees and applicants for employment may raise questions (confidentially, if so requested), discuss potential complaints of discrimination, and on an informal basis, obtain resolution of problems connected with EEO. The EEO counselor serves as a bridge between the complainant and management, and performs a vital function during the initial phase of the complaint process. Additionally, the EEO counselor will:

1. When requested by the DEEOO, conduct an impartial inquiry to gather facts to obtain full understanding of an EEO problem; and/or

2. Seek information from appropriate officials who have direct knowledge relative to the problem presented; and/or

3. Review pertinent records relative to the problem; and/or,

4. Explore with the complainant, management, and the DEEOO ways to resolve the problem; and/or,

5. Keep notes on the counseling sessions, information gathered, and of advice and recommendations. Provide a counselor's report upon the request of the DEEOO after a formal complaint is filed.

b. Training.

(1) EEO Officials. To ensure a result-oriented EEO Program, all EEO officials need to possess basic personnel and EEO program administration skills, knowledge, and capabilities. Knowledge of basic personnel policies and procedures, position management, planning, budgeting, career counseling, human relations, and negotiations necessary for effective management of the program. Participation in conferences and seminars on EEO or civilian personnel related subjects sponsored by the OPM, EEOC, DON, other government agencies, or organizations for women, other minorities, and the disabled, is encouraged and regarded as training experiences. EEO counselors will be provided training in basic EEO and personnel policies and administration the EEOC required course in EEO counseling prior to participating in any counseling session. EEO counselors will attend the EEOC required annual refresher course.

(2) Managers and Supervisors. Managers and supervisors are required to take a minimum of eight hours of EEO training annually. EEO training can be accomplished through attendance at seminars and programs sponsored during Special Emphasis awareness programs or specific EEO classes.

(3) Employees. All employees are required to take annual prevention of sexual harassment training.

16-4. DISCRIMINATION COMPLAINTS

a. General. To help eliminate barriers in order to reach equality of opportunity in all aspects of Federal employment, a complaint system has been established for those who feel they have been discriminated against because of: race, color, religion, sex (including sexual harassment), national origin, age, disability or reprisal. The purpose is to provide a systematic way to promptly, impartially, and equitably resolve discrimination complaints within NCIS. The regulatory requirements and guidelines for processing complaints of discrimination are contained in the DON instruction, Civilian Equal Employment Opportunity Program Management, OPNAVINST 12720.8, 03/22/1990.

b. Applicability.

(1) Any NCIS employee, or, applicant for employment, within NCIS who believes he or she, or a class has been discriminated against must consult with the DEEOO within 45 calendar days of the date of the alleged discriminatory act or personnel action. The DEEOO will assign a counselor who will inquire into the matter and shall attempt to resolve the issue at the lowest management level no later than 30 calendar days after the date on which the matter was called to the counselor's attention by the complainant. Counseling may be extended, only with the

complainant's consent, up to an additional 60 days. If the complainant chooses an alternative dispute resolution process, the period of attempt is 90 calendar days after the date on which the matter was called to the counselor's attention. If the complaint is not resolved within the 30-day time frame, then the complainant has 15 days to file a formal complaint. However, before a formal complaint may be filed, an EEO counselor must counsel the employee. For a diagram of the EEO Complaint Resolution Process, see Appendix 3.

(2) A person alleging discrimination is entitled to a representative of their choice in every stage of the complaint process, including counseling.

c. Responsibility

(1) EADs, ADs, DADs , SACs, ASACs, division chiefs, branch heads, managers and supervisors shall ensure that the EEO Program Policy Statement, Prevention of Sexual Harassment Policy, and the revised EEO Complaint Procedures are posted on official business bulletin boards at all offices within their jurisdiction. The policy statement contains the point of contact person for EEO matters and should be made known to all employees.

(2) The EEO counselor will listen and assist the complainant in specifically identifying the allegation, advising all parties of their rights, and make necessary inquiries. Further, the EEO counselor will make a positive attempt to informally resolve the complaint through discussions with appropriate management officials and through examination of pertinent records.

(3) The DEEOO shall ensure every attempt is made to resolve complaints of discrimination at the lowest possible level, and/or that resolution efforts continue throughout the entire complaint process. For additional information, employees can call the DEEOO at NCISHQ direct.

(4) In the performance of their duties, employees shall extend equal respect, treatment and service to all persons, regardless of race, color, religion, sex, national origin, age, or disability or reprisal. Employees also have an obligation to assist in providing information that can lead to the timely resolution of complaints. Those employees who assist should do so without fear of reprisal, harassment or coercion.

16-5. AFFIRMATIVE EMPLOYMENT PROGRAM

NCIS follows the DON AFFIRMATIVE EMPLOYMENT PROGRAM**.**

16-6. EEO INSPECTION

a. General.

(1) To meet the requirements of OPNAVINST 12720.8O and DON instruction, Equal Employment Opportunity Program Management, OPNAVINST 12720.4B, 07/11/1989, periodic in-depth EEO Program reviews are scheduled during command inspections/visits.

(2) The NCIS DEEOO, or an EEO representative will conduct the review. The purpose of the review is to determine the level of management and supervisory commitment and support for the EEO Program, employee attitudes, patterns and trends in employment practices, and problems facing managers in their efforts to promote and implement the EEO Program.

b. Purpose. Meaningful and measurable criteria has been established to monitor and evaluate the total EEO Program with positive action being initiated based on the findings of the NCIS Field Office review. Program compliance and effectiveness covers areas relating to EEO for civilian personnel. This includes all aspects of personnel management, recruiting, hiring, training, promotion, disciplinary actions, sexual harassment, and working conditions. Personnel shall be managed without regard to race, color, religion, sex, age, national origin, disability or reprisal. Upon completion of the NCIS Field Office EEO Program review, the DEEOO will inform the NCIS Inspector General (Code 00I) of specific items of interest which should be examined. The DEEOO will also provide the SAC and the Director, NCIS with an assessment of the NCIS Field Office EEO Program effectiveness. In addition, a written report will be submitted to the Inspector General with a recommended grade and a summary of conditions.

APPENDIX 1: NCIS EQUAL EMPLOYMENT OPPORTUNITY POLICY

EQUAL EMPLOYMENT OPPORTUNITY POLICY

January 20, 2006

I am personally committed to promoting equal employment opportunity for all persons in the workplace. All individuals at NCIS as well as applicants, regardless of race, color, age, sex, religion, national origin, or disability will be assessed only on the basis of their individual merit and ability to get the job done.

Secretary Donald Winter has said that people are our most valuable asset. I most heartily agree with and support that principle. In order to take full advantage of this valuable asset, we must be inclusive and respectful of all groups of individuals to attain and retain the best of the best for NCIS. Each employee of NCIS is an integral part of fulfilling our mission as an innovative, initiative oriented professional law enforcement and security agency. Each of us must be sensitive to our cultural differences and value the contributions each member makes to the accomplishment of our mission. For our managers and supervisors, both military and civilian, establishing and maintaining a sound equal opportunity environment are integral to their job. NCIS will provide a work environment free of harassment and discrimination of any kind. We must all do our part. I am confident that continued support of this policy throughout NCIS will demonstrate an inclusive and fair work environment that compliments our noble mission. Anyone having questions regarding our EEO posture and/or policy is encouraged to discuss them
directly with me or with my Deputy EEO Officer, (b)(6) who may be reached on (b)(6) (b)(6)

/S/

(b)(6)
DIRECTOR

APPENDIX 2: NCIS SEXUAL HARASSMENT POLICY

SEXUAL HARASSMENT POLICY

June 7, 2006

Sexual harassment is unacceptable conduct and will not be tolerated. Sexual harassment is a form of sex discrimination and is an "unlawful employment practice" under Title VII of the Civil Rights Act of 1964, as amended. SECNAV Instruction 5300.26D of 3 January 2006 is the Department of the Navy policy on sexual harassment.

Sexual harassment is defined in law and regulation as unwelcome sexual advances, requests for sexual favors, and other verbal or physical conduct of a sexual nature. Sexual harassment can occur when (1) submission to such conduct is made either explicitly or implicitly a term or condition of an individual's employment (i.e.: must be tolerated to maintain employment); (2) submission to or rejection of such conduct by an individual is used as the basis for employment decisions affecting the individual (i.e.: promotions, assignments, etc.); or (3) such conduct has the purpose or effect of unreasonably interfering with an individual's work performance or creating an intimidating, hostile, or offensive working environment.

There are two main types of sexual harassment: (1) Quid Pro Quo or "this for that." Quid Pro Quo occurs when employment decisions such as hiring, promotions, salary increases, work assignments, or performance evaluations are based on an employee's willingness to grant or deny sexual favors; and (2) Hostile Work Environment, which is the most subtle form of sexual harassment. Hostile Work Environment can occur when behavior in the work place focuses on the sexuality of another person or occurs because of the person's gender. Such workplace behavior can include statements, actions, non-verbal actions (i.e. leering, making gestures), physical contact, or audio/ visual media displays (i.e. posters, photographs and screen-savers). All forms of sexual harassment refer to behavior that is not welcome, personally offensive, and/or debilitates morale.

Preventing sexual harassment is the responsibility of every member of this agency. Individuals who believe that they have been sexually harassed are encouraged to address their concerns or objections regarding the incident directly with the person demonstrating the harassing behavior. Persons who are subjected to, or, observe objectionable behavior should promptly notify the chain of command if:

(1) The objectionable behavior does not stop; and/or,

(2) The situation is not resolved; and/or,

(3) Addressing the objectionable behavior directly with the person concerned is not reasonable under the circumstances; and/or,

(4) The behavior is clearly criminal in nature.

If the person demonstrating the objectionable behavior is a direct superior in the chain of command or the chain of command condones the conduct or ignores a report, individuals who have been subjected to or who observe objectionable behavior are encouraged to promptly communicate the incident through other available means. Employees can contact the Equal Employment Opportunity Officer, who will provide assistance and guidance. Employees can also report the conduct to the NCIS Inspector General's Office.

It is the responsibility of management to investigate allegations of sexual harassment and take necessary action to ensure such allegations are addressed swiftly, fairly, and effectively. NCIS handles reports of sexual harassment promptly and fairly. Managers and supervisors must be aware of what constitutes sexual harassment in order to explain the sanctions for violations, and address matters brought to their attention.

Supervisors must set the example in treating all employees with dignity and respect, fostering a climate free from all forms of unlawful discrimination including sexual harassment in the work environment. Supervisors are responsible for and must be committed to preventing sexual harassment in the work environment. Supervisors must not ignore or condone sexual harassment in any form. Reprisal against individuals who report sexual harassment is prohibited. Supervisors must take whatever action is required to ensure that an individual subjected to sexual harassment is not subsequently subjected to reprisal or retaliation by the alleged perpetrator or peers of the complainant.

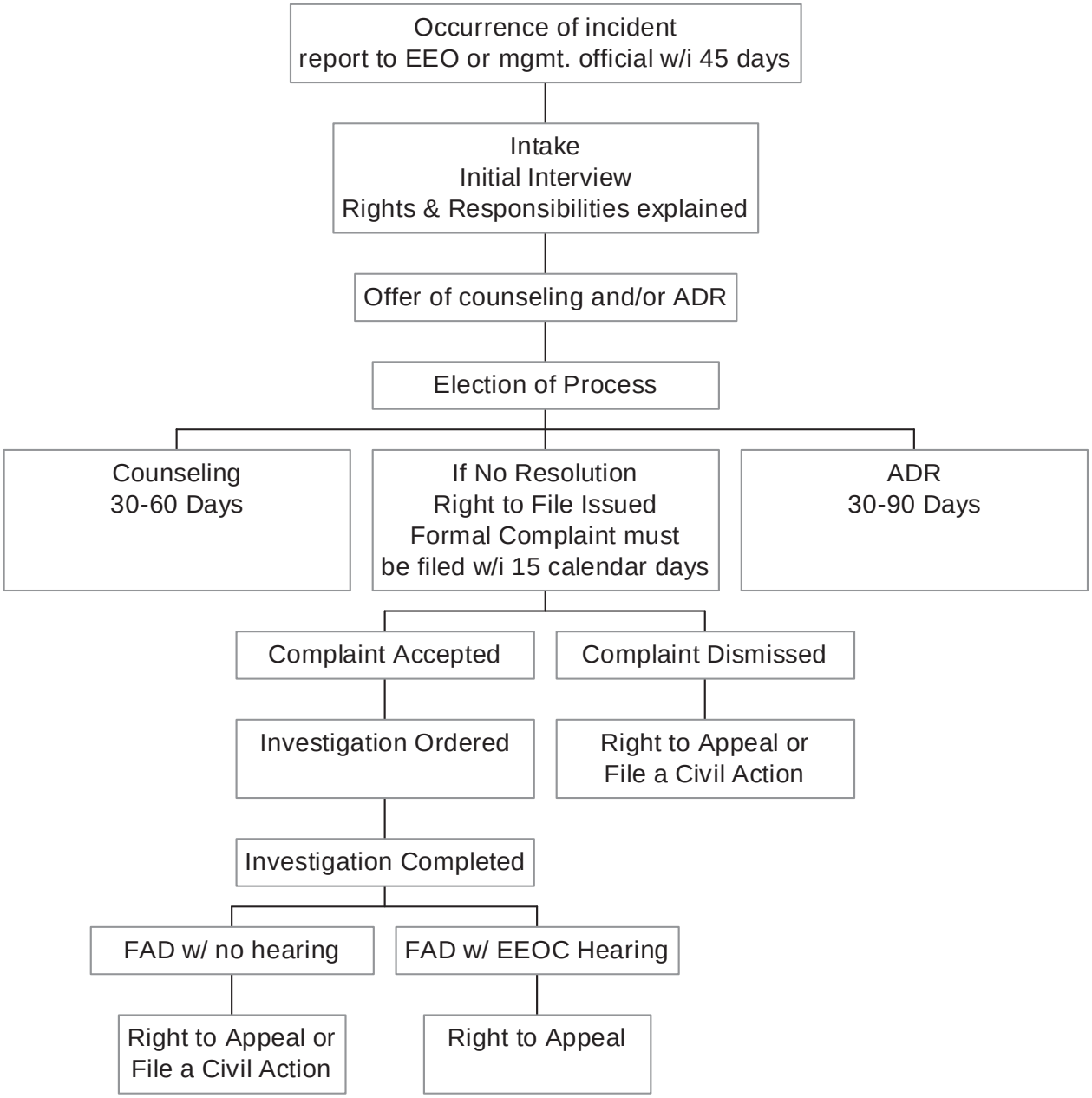
All agency employees must annually complete the online training module for the Prevention of Sexual Harassment at: http://training.newmedialearning.com/psh/usnshhro/index.htm. Please complete this course if you have not done so within the last 12 months. The Equal Employment Opportunity Office monitors course compliance.

I expect each of you to do your part. If you have any questions or concerns regarding this policy, please contact the Deputy EEO Officer, Ms. (b)(6) or by email at (b)(6)@ncis.navy.mil.

/S/

(b)(6)

APPENDIX 3: EEO COMPLAINT RESOLUTION PROCESS



CHAPTER 17
TITLE: ADMINISTRATIVE GRIEVANCE SYSTEM
POC: CODE 10A
DATE: DEC 06

17-1. GENERAL

This chapter establishes the Naval Criminal Investigative Service (NCIS) Administrative Grievance System (AGS). The NCIS AGS complies with Department of the Navy Human Resources (DONHR) Implementation Guidance 771-01 and DOD Civilian Personnel Manual 1400.25-M, Subchapter 771.

17-2. PURPOSE

To provide a fair, equitable and timely forum for the review and resolution of disputes regarding employment-related matters, and to establish a systematic method for the employee to seek personal relief in matters of concern or dissatisfaction. All persons involved in the dispute resolution process shall be free from restraint, interference, coercion, discrimination, or reprisal.

17-3. POLICY

The NCIS AGS incorporates the procedures set forth in DONHR Implementation Guidance 771-01 NCIS specific procedures and a brief outline of the AGS process are provided as follows:

a. Filing an Administrative Grievance. Employees should attempt to resolve workplace grievances on an informal basis with their immediate supervisor. If this fails, administrative grievances may be filed at the appropriate level of the chain of command consistent with the decision authorities outlined below.

b. Decision Authority. In view of the widespread geographical dispersion of NCIS components, as well as the centrally directed nature of the organization, the administrative grievance procedure will incorporate three specific levels of decision authority as follows:

(1) NCIS Resident Agency (NCISRA) Level. Limited to those grievances which would be strictly local in nature and over which the Supervisory Special Agent (SSA) would have cognizance and control. They would include, for example, working conditions and hours of work.

(2) NCIS Field Office (NCISFO) Level. Limited to those matters in which the Special Agent in Charge (SAC) would have cognizance and ability to resolve or adjudicate.

They may include such issues as NCISFO directed work rules, NCISFO policy, Temporary Duty (TDY) assignments and, in general, those problems and circumstances resolvable by the NCISFO.

(3) NCIS Headquarters (NCISHQ) Level. In addition to working conditions and grievable situations within NCISHQ, this level would include all matters subject to NCIS-wide policy and matters not suitable to be resolved at the NCISRA or NCISFO levels.

c. Grievance File. The completed grievance file will be maintained by the NCIS Personnel Operations and Services Department, Code 10A, for four (4) years. The file will contain documents or copies of documents relating to the grievance.

CHAPTER 18
TITLE: DISCIPLINE AND ADVERSE ACTION PROCEDURES
POC: CODE 10A
DATE: MAY 08

18-1. INTRODUCTION

This Chapter establishes the policies and procedures for proposing and effecting disciplinary and adverse actions against civilian employees of the Naval Criminal Investigative Service (NCIS). The procedures outlined in this chapter comply with the requirements the Department of the Navy (DON) Civilian Human Resources Manual (CHRM) Subchapter 752, Disciplinary Actions, with the exception of specific items outlined in paragraph 5 below.

18-2. PURPOSE

To provide managers and supervisors guidance in using discipline as a managerial tool to correct deficiencies in employee behavior and attitude, and correct situations which interfere with efficient operations of the NCIS.

18-3. DEFINITIONS

The definitions applicable to this policy can be found in DON CHRM Subchapter752. For purposes of this chapter, 'Activity' as used in Subchapter 752 is defined as a field office or headquarters code.

18-4. POLICY

It is the policy of the NCIS to impose the minimum penalty that can reasonably be expected to correct the employee's conduct and to maintain efficiency, discipline, morale and integrity within NCIS. However, as the DON primary investigative service, with a wide range of jurisdictional responsibilities for which NCIS is accountable to the public, it is imperative that a policy of strict discipline be applied within NCIS.

18-5. DISCIPLINARY PROCEDURES AT NCIS

a. Special Agents in Charge (SAC) and Deputy Assistant Directors (DAD) are authorized to approve first-level disciplinary actions including Oral Admonishments and Letters of Caution. These actions are neither grievable nor appealable and will not be made a matter of record in an employee's official personnel folder.

(1) An Oral Admonishment is a counseling session in which the supervisor advises an employee of a shortcoming, infraction of rules, or unacceptable performance or conduct, and includes required corrective action. Situations which call for oral admonishment may include improper absenteeism, sick leave usage, extended breaks or lunch periods, conduct which infringes on other employees' rights, or failure to perform certain assigned tasks. The employee is counseled that further disciplinary action may be imposed for continued deficiencies.

(2) A Letter of Caution is a written notification of unacceptable conduct which warns the employee that a disciplinary action may be imposed unless the conduct improves. Situations which may call for a Letter of Caution are similar to those listed above for an Oral Admonishment. The Letter of Caution serves to establish that the matter has been brought to the employee's attention and that the appropriate standard of conduct or performance has been communicated to the employee. Although a letter of caution is not placed in the employee's official personnel folder, the issuing supervisor retains a copy as evidence that the employee has been counseled. This form of corrective action is usually employed for minor infractions or deficiencies when past discussions or counseling have not achieved their purpose. A sample Letter of Caution is attached at Appendix (1).

(3) Reporting Requirements. To ensure uniformity of disciplinary actions within NCIS, Oral Admonishments and Letters of Caution will be reported quarterly to Code 10A2. Reports should not include employees' names. Quarterly reports should be submitted no later than the tenth working day of the month following the end of the quarter. Quarterly reports will not be retained in official personnel files or any system of records from which data is retrievable by name or any other personal identifier. Code 10A will not retain the original reports once review and statistical compilation are complete. A sample quarterly report is included at Appendix (2).

b. The DAD for Personnel Operations and Services (Code 10A) will serve as the Proposing Official for all covered actions for which an employee may file an appeal with the Merit Systems Protection Board (MSPB) or a grievance under the Administrative Grievance Procedures of NCIS-1, Chapter 17.

(1) Disciplinary actions, which may be grieved using the procedures described in NCIS-1 Chapter 17, include a Letter of Requirement, a Letter of Reprimand, and a suspension for 14 days or less.

(a) A Letter of Requirement is a written notification, or order, issued to an employee concerning conduct deficiencies, which clearly establishes requirements and procedures to be followed by the employee to avoid a future disciplinary action. Although it is not made a matter of record in the employee's official personnel file, a letter of requirement may be retained by the

supervisor for a period not to exceed one (1) year. A sample Letter of Requirement is attached at Appendix_(3).

(b) A Letter of Reprimand records and communicates to the employee specific information on unacceptable conduct. It usually follows previous attempts to correct conduct deficiencies such as counseling, oral admonishment, or a letter of caution. A copy of the letter of reprimand will be retained in the employee's official personnel folder for a period of two (2) years. During this period, the Letter of Reprimand may be considered when determining disciplinary action to be taken for other offenses.

(c) A suspension of 14 calendar days or less means placing an employee, for disciplinary reasons, in a status without duties and without pay. Suspensions must be for consecutive calendar days. A suspension occurring before or after a holiday does not have any affect on holiday pay. However, a holiday occurring during a period of suspension must be counted as part of the suspension.

1. A suspension of 14 days or less entitles the affected employee to advance written notice of the action. The notification letter will state the specific reason(s) for the proposed action; the name and title of the designated deciding official; the amount of time (normally 15 calendar days but not less than 24 consecutive hours) that the employee is allowed to provide an answer orally and/or in writing; and the right to review, or have a representative review, the material relied upon to support the proposed action.

2. The employee is entitled to a reasonable amount of official time to review the notice and supporting material; secure affidavits; answer orally and/or in writing; and be represented by an attorney or other representative. An employee may request an extension of the time necessary to reply. The designated deciding official will grant or deny such an extension in writing to the employee.

3. Decisions on suspensions of 14 days or less will be made at or above the Assistant Director level. The employee will be provided a written decision as soon as possible after the employee's reply deadline has elapsed. The decision letter will consider any answer or information provided by the employee and/or his/her representative; specify the reason for the decision; identify any grievance procedures available to the employee. If the decision letter upholds the proposed suspension, the letter will be delivered to the employee on or before the effective date of the suspension.

4. The starting date of a suspension is at the discretion of the deciding official. Although the action is grievable under the administrative grievance procedures, suspensions of 14 calendar days or less are not appealable to the MSPB.

(2) Disciplinary actions which may be appealed to the MSPB include suspensions of more than 14 days, indefinite suspensions, demotions (reduction in grade or pay), furloughs for 30 calendar days or less; and, removals.

(a) The procedures for effecting appealable adverse actions are very similar to those used for suspensions of 14 calendar days or less. Normally, the employee is provided 15 calendar days, but not less than seven (7) days, to reply personally and/or in writing to the deciding official in the matter. The Deciding Official will review the recommended action independently and evaluate the employee's reply. The Notice of Decision will be issued to the employee any time after the reply period expires, but normally not later than 30 calendar days after the employee receives the advance notice. The action will be effected no earlier than 30 calendar days after the employee's receipt of the notice of proposed adverse action. The Deciding Official will provide a written report of their final determination to Code 10A, who will ensure proper filing of documents in the employee's official personnel file and/or departmental files.

(b) In emergency situations, an employee may be excused from duty without charge to leave or loss of pay during the 30-day notice period of a removal or indefinite suspension when the circumstances are such that retention of the employee in an active duty status during the notice period may be injurious to the employee, fellow workers, or the general public; may result in damage to government property; may impede the efficiency of operations; or, because the nature of the employee's offense reflects unfavorably on the public perception of the DON or NCIS.

(c) NCIS may take action with a shortened notice period of not less than seven (7) days when there is reasonable cause to believe the employee committed a crime for which a sentence of imprisonment may be imposed.

(3) Appeal Rights. Excepted Service employees who have 1 year or more of continuous service may appeal a covered action to the MSPB. An appeal may be submitted at any time after receipt of the decision letter, but no later than 30 calendar days after the effective date of the action. The employee will be advised of this right in the decision letter and also that the employee's appeal to the MSPB must be in writing and should furnish reasons for contesting the adverse action together with any offer of proof and pertinent documents the employee is able to submit.

(4) Variance from Procedures. The administrative procedures described herein or in CHRM Subchapter 752, shall be routinely followed. However, at the Director’s discretion, these procedures may be altered in any case containing circumstances determined to justify a variance.

APPENDIX (1): SAMPLE LETTER OF CAUTION

From: (Title, Activity)
To: (Name, Title)

Subj: LETTER OF CAUTION

Ref: (A) NCIS-1, Chapter 18

1. This letter serves to admonish you for (NATURE OF OFFENSE), as detailed below:

a. (GIVE SPECIFICS)

b. On (DATE), I personally discussed the above situation with you and emphasized the need for correction.

2. A copy of this letter will be retained by me for a period not to exceed 1 year. This letter is temporary in duration and will not be filed in your official personnel folder. Further, the action which prompted this letter will not serve as a prior offense in determining a remedy in accordance with reference (a) should future disciplinary action be deemed necessary.

3. This letter is being issued to improve the situation at hand. It is neither grievable nor appealable under established procedures.

_____
(Signature)

I acknowledge receipt of this notice on (Date)

_____
Employee Signature

APPENDIX (2): SAMPLE QUARTERLY REPORT

From: SAC, (Field Office) or Deputy Assistant Director (Department)
To: Code 10A2 (Employee Relations)

Subj: QUARTERLY REPORT OF ORAL ADMONISHMENTS/LETTER OF CAUTION

Ref: (A) NCIS-1 Chapter 18

1. Per reference (a), the following information is provided for statistical purposes, to ensure consistency of discipline, and to review potential training issues within NCIS:

Reporting Period: _____ (indicate Jan-Mar, Apr-Jun, Jul-Sep, Oct-Dec)
Number of Oral Admonishments Issued: _____
Number of Letters of Caution Issued: _____

A brief synopsis of the behavior/action generating each oral admonishment or letter of caution should be attached. Example: Oral Admonishment - Clerical employee left for lunch without ensuring adequate phone coverage.

Example: Letter of Caution - Special Agent failed to promptly turn in evidence.

Employee's name should not be included in the report.

SIGNATURE: _____

Typed or printed name: _____ Date:_____

APPENDIX (3): SAMPLE LETTER OF REQUIREMENT

From: (Title, Activity)
To: (Name, Title)

Subj: LETTER OF REQUIREMENT

Ref: (a) NCIS-1, Chapter 18
(b) NCIS-1, Chapter 17

1. The purpose of this letter is to place a requirement upon you with regard to (briefly state the requirement; e.g., requesting leave, etc.). The reason(s) for the imposition of this requirement and the accompanying details are specified below:

a. (Specify in detail why the requirement is being put into effect, giving specific dates where appropriate, and cite the details of the requirement.)

b. On (date) I personally discussed the above with you, and at that time informed you of the requirement that would be placed upon you. (Discussion should be held with the employee prior to the issuance of a letter of requirement. At that time the employee should be informed that he/she is to receive a letter of requirement and the reason(s) therefore.)

2. A copy of this letter will be retained by me for a period not to exceed one (1) year. This letter does not effect a formal disciplinary action, is temporary in duration, and will not be filed in your official personnel folder. Further, the action which prompted this letter will not serve as a prior offense in accordance with reference (a) should future disciplinary action be deemed necessary.

3. This informal action is being taken for the purpose of bringing to your attention a situation for which you must take positive steps to correct. It is anticipated that you will respond properly. You may grieve this letter under the established administrative grievance procedures set forth in reference (b). If you decide to pursue a grievance, you must initiate the action within 15 calendar days of your receipt of this letter. You may contact (Name, Title, Servicing Personnel Activity, Telephone Number) for assistance with the grievance procedure.

_____
(Signature)

I acknowledge receipt of this notice on (Date)

_____
Employee Signature

CHAPTER 19
TITLE: FILE RETENTION AND DISPOSAL OF CLOSED INVESTIGATIONS, OPERATIONS, SOURCES AND SECURITY CLEARANCE ADJUDICATION CASES
POC: CODE 11C1
DATE: SEP 08

19-1. GENERAL

19-1.1. The Naval Criminal Investigative Service (NCIS) Headquarters (NCISHQ) Investigative and Operational Records Management System (RMS), described in this chapter, was developed to provide for systematic retention and retrieval of all NCIS investigative, counterintelligence, counterterrorism, and Security Clearance Adjudication closed case files. RMS was designed to ensure that only pertinent and substantive material is held in the NCIS Records Management Branch (RMB) Records Center and that files are held in accordance with retention and disposition criteria approved by the Archivist of the United States and published in SECNAV Manual 5210.1, Records Management Manual, or on an approved Standard Form 115 (SF 115), Request for Records Disposition Authority. Only records designated below, and having retention periods of five years or longer, will be stored in the RMB Records Center. This chapter also addresses records indexed in the Defense Central Index of Investigations (DCII). DCII serves as the master index to the records maintained in the NCIS RMB, Records Center and conforms to provisions of Department of Defense (DoD) Regulation 5200.2-R, Personnel Security Program, Chapter XII and DoD Instruction 5505.7, Titling and Indexing Subjects of Criminal Investigations in the DoD.

19-1.2. Governing federal statutes and instructions mentioned in this chapter include: SECNAV Manual 5210.1, Records Management Manual (Part III), DoD Regulation 5200.2-R, Personnel Security Program, Chapter XII, DoD Directive 5200.27, Acquisition of Information Concerning

Persons and Organizations not Affiliated with the DoD, and DoD Directive 5240.1, DoD Intelligence Activities.

a. The RMB is responsible to maintain, control, and manage NCIS closed case files and accomplish the disposal of these records in accordance with guidance for each specific record series as contained in SECNAV M-5210.1. Closed cases managed by RMB include all NCIS investigative and select counterintelligence and counterterrorism operational records. RMB also serves as Department of the Navy's (DON) central records center for criminal investigations, United States Marine Corps (USMC) and Criminal Investigation Division (CID) investigations, incident reports (IR) created by Navy law enforcement (i.e., GENCRIM) and USMC Provost Marshal offices, and the DON Central Adjudication Facility (DON CAF) personnel security adjudication case files. Closed cases held by RMB are the official copy of record. Copies held in the field, as defined by SECNAV M-5210.1, have expired or extended retention requirements are considered additional copies and should be destroyed upon authorization.

b. Contents of this chapter do not pertain to files retained for administrative purposes. Policy for administratively retained files is contained in SECNAV M-5210.2, Standard Subject Identification Codes (SSIC), and SECNAV M-5210.1.

19-1.3. The following tables provide a breakdown of retention periods applied to the various types of investigative, operational, and collection reporting received at the NCISHQ RMB and stored in the Records Center. The schedule is broken out by applicable SSIC and case category codes. SECNAV M-5210.1 contains official retention and disposition guidance for DON records. There are several disposition guidelines pertinent to NCIS law enforcement (GENCRIM), counterintelligence, counterterrorism, and computer investigations and operations (CI/CT/CYBER) records that are not in, or not correctly cited, in the current edition of the SECNAV manual. The U.S. National Archivist, however, has granted approval, and the records of these additions and/or changes are on file in the NCIS RMB. The following matrices are offered to provide summarized lists of NCIS records that have been approved. Note that some case categories cited in the matrices are not in current use; however, numerous records created under these obsolete category codes still exist and are stored in the Records Center. These matrices are included to serve as retention and disposition guidance for RMB personnel as well as for informational guidance to potential NCIS customers. Questions regarding records management can be directed to the Head or Assistant Head of the RMB. A summary of the retention periods for CI/CT/CYBER law enforcement investigations and operations, STAAT operations, and NCIS personnel investigations and security clearance adjudications cases is contained below:

a. Counterintelligence/Counterterrorism Records (SSIC 3850): See Appendix (1).

b. Inspection Records (SSIC 5522): See Appendix (2).

c. Personnel Investigative Records (SSIC 5527): See Appendix (3).

d. Law Enforcement Records (SSIC 5580): See Appendix (4).

19-1.4. The DON CAF is responsible for adjudicating the clearance eligibility of Navy and Marine Corps military and civilian personnel for access to classified information and adjudicates the sensitive compartmented information access eligibility for DON military and civilian personnel (there are some files pertaining to Coast Guard personnel remaining from the period when DON CAF was responsible for their adjudicative actions). Derogatory adjudicative material, to include denial, revocation or other unfavorable administrative actions, which are not part of other files (BUPERS/HQMC), are made a part of the NCISHQ file system and retained. Personnel Security Clearance Adjudication case files (SSIC 5529) are retained as shown in Appendix (5).

19-1.5. Additional security clearance adjudication material created after the creation of the case file in RMB will be added to the existing case file. The disposal date is 25 years from the date of the latest adjudication material.

19-2. NON-DEPARTMENT OF DEFENSE AFFILIATED PERSONS AND ORGANIZATIONS

19-2.1. DoD Directive 5200.27, 'Acquisition of Information Concerning Persons and Organizations not Affiliated with the DoD', provides general policy on DoD command collection, retention, and dissemination of information on persons and organizations not affiliated with the DoD in the U.S. and on non-DoD affiliated U.S. citizens anywhere in the world.

19-2.2. However, DoD Directive 5200.27 is not applicable to DoD intelligence components as they are defined in DoD Directive 5240.1. DoD 5240.1, 'DoD Intelligence Activities', and DoD 5240.1-R, 'Activities of DoD Intelligence Components that Affect U.S. Persons', are the only authorities used as guidance by DoD intelligence components to collect, retain, or disseminate information concerning U.S. persons. The counterintelligence elements of NCIS are DoD intelligence components and the Director, NCIS directs, manages, and controls execution of all DON CI functions, except those within the responsibility of the Marine Corps Director of Intelligence under SECNAVINST 3850.2C.

19-2.3. DoD 5200.27 also does not apply to criminal investigations. Criminal investigations in DoD are governed by the DoD Directives and Instructions in the 5505 series. Under SECNAVINST 5430.107, the Director, NCIS is the senior official for criminal investigations in DON.

19-2.4. The provisions of DoD Directive 5200.27 encompass the authorized activities that justify acquisition of information on non-DoD affiliated persons and organizations, or non-DoD affiliated U.S. citizens anywhere in the world, and are among the primary responsibilities of NCIS under SECNAVINST 5430.107 and SECNAVINST 3850.2C. Commands should not be collecting such information, unless it is for a criminal investigation, and NCIS has declined investigative jurisdiction.

19-2.5. Under no circumstances will information be acquired about a person based solely on the exercise of his or her First Amendment rights, such as lawful advocacy of measures in

opposition to government policy.

19-3. COUNTERINTELLIGENCE (CI) MATTERS

Executive Order 12333, entitled U.S. Intelligence Activities, defines counterintelligence (CI) as information gathered, and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities, but not security programs pertaining to personnel, physical, document, or communication security programs. The essence of this definition is that CI is directed against a foreign threat, which includes those U.S. persons, where reason to believe exists, that they are acting as agents for foreign powers, persons or organizations in the activities specified above. DoD Directive 5240.1, "DoD Intelligence Activities", which implements Executive Order 12333 for DoD, states that the counterintelligence elements of the NCIS are included within the listing of DoD Intelligence Components (DoDIC). DoD Directive 5240.1, its guiding regulation, DoD 5240.1-R and SECNAVINST 3820.3E, Oversight of Intelligence Activities within the DON, each expressly state that they do not apply to law enforcement activities. Procedure 3 of DoD Regulation 5240.1-R provides that CI information regarding U.S. persons that was properly collected (in accordance with Procedure 2.) and relevant to the authorized missions of the DoDIC concerned may be retained.

19-4. ACCESS, RETENTION AND DISSEMINATION OF CI/CT/CYBER INFORMATION

19-4.1. Access within NCISHQ to CI/CT/CYBER information about U.S. persons shall be limited to those with a need to know.

19-4.2. CI/CT/CYBER information is retained in accordance with paragraph 19-1.2.a. of this chapter. The following additional guidelines are provided:

a. Information regarding U.S. persons that pertains solely to the functions of other DoD components or agencies outside DoD shall be retained only as necessary to transmit or deliver such information to the appropriate recipients.

b. Information about U.S. persons may be retained temporarily by the collecting activity, for a period not to exceed 90 days, solely to determine whether that information may be appropriate for further retention. This material is never sent to RMB for storage.

c. Information about U.S. persons that was improperly collected shall be retained only for the reporting of such collection for intelligence oversight purposes and for any later proceeding that may be necessary.

19-4.3. CI information on non-military U.S. persons disseminated to USN and USMC commands shall be designated for return to NCIS within 30 days. Dissemination of such information to elements of the U.S. intelligence, law enforcement, and security community shall not contain retention guidelines, as each agency is required to make its own determination.

19-5. FIELD OFFICE (FO)/ RETENTION AND DISPOSAL

19-5.1. Control Case Documentation. In every control case, the field office (FO) shall receive one copy of the Report of Investigation (ROI) (OPEN) submitted by the NCIS Resident Agency (NCISRA) or Resident Unit (NCISRU). Retention of the Director's Special Interest (DSI) and Special Interest (SI) investigations by the FO will not exceed the pendency of the investigation. At the discretion of the Special Agent in Charge (SAC), documentation may be held in extended retention after the case is closed to facilitate matters responsive to specific taskings by senior persons, and other materials judged to be of substantive value to the FO. Authorization of extended retention must be documented on the Case Tracking and File Management Form (NCIS 5580/54) and maintained within the case file. Materials held beyond the pendency of the investigation must be periodically reviewed to ensure that unnecessary documentation is not being maintained. For information regarding the retention and disposal of source records, see the guidelines set forth in NCIS-3, Chapter 8, Central Source Registry.

19-5.2. Lead Case Documentation. The control FO will be included on distribution for all leads generated by the NCISRA/NCISRU. Lead offices responding to taskings will include the FO on distribution for all case documentation, including exhibits, when the FO is identified by the control office in the distribution section of the ACTION/LEAD. It is considered unnecessary and duplicative for the FO to maintain lead case materials. Leads should be maintained for 90 days by the FO for all investigations and operations. Leads may be automatically destroyed after the 90 days. Leads are maintained by the control office in the master case file and do not meet the automatic destruction criteria.

19-5.3. ROI (INFO) (formerly NCIS Operations Reports (NORs)) and Intelligence Information Reports (IIRs).

a. The ROI (INFO) that documents criminal or counterintelligence activity collected on an opportunity basis is destroyed in accordance with the retention of the particular case category the subject thereof is incorporated into the CCS 2000, (see Section 19-6. below). An ROI (INFO) not constituting a substantive addition to the FO file holdings should be destroyed after confirmation that records are located at RMB Finished Files.

b. ROI (CLOSED) "ONLY REPORTS" and ROI (INFO) reports will be mailed/sent to RMB with the appropriate current Records Information Management System (RIMS) cover sheet. This is applicable to both ROI (INFO) and ROI (CLOSED) "ONLY REPORTS" that either have or do not have exhibits, with exception for cases designated DSI/SI, 3C, 5T, XXCE, XXCT and 7H (see paragraph 19-8.1.e.(2)).

c. Copies of NCIS produced IIRs may be retained by the preparing office, or other NCIS field element with an interest in the information provided, for one year. Extended retention is provided via the DIA InfoSphere Management System (ISM) and PORTICO databases.

19-5.4. Other Agency Reports. A report that the FO receives from other federal and non-federal law enforcement and security agencies will generally relate to cases in which the NCISHQ has an interest. With the exception of a report received from a police (federal, state and local)

department, and in a case worked jointly with another agency (federal, state, and local), the report should not be filed with the basic case. The police report should be summarized within the NCIS investigative report. A report published by another agency may be appended to NCIS reports where that agency grants written permission. When other agency reports do not pertain to NCISHQ investigations but are furnished for information, or advisement of appropriate commands, and are germane to NCISHQ mission and functions, the reports may be retained for one year and incorporated into the Case Control System 2000 (CCS 2000).

19-5.5. Additional Field Office Files.

a. FO operational files represent the FO's investigative and counterintelligence database and shall be the only files used for case documentation and related material.

b. The FO may accumulate material that does not lend itself to inclusion into these files. This material includes, but is not limited to, intelligence publications, local collection requirements, port security matters and various counterintelligence or security studies. The latter would include monographs, analyses and briefs whether produced by NCISHQ or another agency. This material may be disposed of (i.e., destroyed) when it is no longer needed. In order to ensure that such material is not maintained beyond its necessary period of retention, it shall be retained together in a separate file (either electronic or hardcopy) titled "Miscellaneous Operational Files". It is incumbent upon supervisory personnel to review these holdings regularly to make certain that appropriate purging is accomplished.

19-6. FIELD OFFICE CCS 2000 (also known as MASTER NAME INDEX)

19-6.1. Master name information from the title block is entered into the automated CCS 2000 database for all control cases, certain ROI (INFO), lead cases, and other operational documentation which warrants, and is authorized, retention for one year, and, as previously stated, will normally be destroyed when the investigation is determined to be in RMB Finished Files. The FO CCS 2000 exists to provide the FO with a working index for investigative and operational files.

19-6.2. When a file is destroyed that had been maintained in the FO file retention program, the CCS 2000 entry supporting that case file will also be deleted. In situations wherein the FO determines that a particular file warrants extended retention, and is authorized for retention, a new destruction date must be entered into the CCS 2000 database. (See the CCS 2000 User Guide located on the NCISnet under Guides and Manuals.)

19-7. FIELD OFFICE AND NCIS RESIDENT AGENCY FILES

The responsibility for management of FO case files rests within the investigative support side of the FO. In order to support the disposal process, FO files shall be arranged alphabetically and CCS 2000 entries should contain an annotation specifying the closing date of each file.

19-8. FIELD OFFICE AND NCISRA FILE RETENTION, SUBMISSION TO NCISHQ AND DESTRUCTION

19-8.1. The FO and NCISRA are the primary field repositories for closed investigations and operations. The FO and NCISRA are authorized to maintain only those files, records, and publications necessary for the accomplishment of their mission. Procedures for control, submission of finished file cases to NCISHQ, and purging of closed or other extraneous operational material are outlined below:

a. Retention. The FO and NCISRA shall retain files on closed investigations, operational and collection matters to include specific phase Polygraph Examination cases for a period not to exceed one year as prescribed in SECNAV M-5210.1. At the field level, this includes Agent Notes and other material (e.g., original correspondence). Exceptions include the following: cases awaiting judicial, administrative, or appellate action; referrals to other agencies; approved characterizations; IIR or ROI (INFO) reporting information of long term counterintelligence, domestic security or criminal investigative interest to the component involved, which warrant, and are authorized extended retention. These must be maintained in "Extended Retention" files. For CI/CT/CYBER cases, a case with a "/F" disposition code shall not be destroyed until a ROI (DISP) has been prepared for each Subject, Co-Subject, or Company indexed as a master or secondary title (NCIS-1 Chapter 25, paragraph 25-5.9 applies) and, for GENCRIM cases, CLEOC entries are made. Additionally, case files should not be destroyed prior to the disposal of active evidence.

b. File Arrangement (One-Year Files) and Disposition. FO and NCISRA one-year files on closed material shall be arranged alphabetically. This material must be purged immediately upon expiration of the authorized retention period, preferably on a monthly basis. CCS 2000 periodic reports provide a listing, in alphabetical order, of all material requiring destruction. The alphabetic listing of cases to be destroyed should be properly annotated to determine which records will be purged from the database and which records will be put into extended retention. Computerized case control entries should be purged from the database at the time case material is destroyed.

c. File Arrangement (Extended Retention Files). Material that meets the criteria for extended retention beyond one year must be physically separated from the one-year files, in a section marked "Extended Retention", and filed alphabetically. In each instance, the computerized case control entry shall include the "Extended Review Date", defined as the date that the specific case material will be reviewed for destruction or continued in extended retention. CCS 2000 includes a function that automatically lists all material in extended retention alphabetically along with the date that the material is to be reviewed. The SAC is responsible for reviewing the extended retention list periodically (at a minimum, semi-annually) to ensure that material is destroyed when it has served its purpose or when the authorized retention period expires.

d. Retention of Counterintelligence/Counterterrorism Material Beyond One Year.

(1) The FO may have legitimate requirements for retaining certain miscellaneous counterintelligence type documentation for more than one year. This material includes local collection requirements, port security matters, intelligence publications, and various counterintelligence, counterterrorism, security, or investigative production efforts. This material

should be retained separately.

(2) Upon conclusion of a CI, CT, or CYBER investigation or operation, documentation pertaining to it shall be destroyed within one year after confirmation of receipt from Code 11C12, unless a request is received from the NCISHQ cognizant code that it is to be forwarded elsewhere.

(3) The NCISRA is authorized to retain certain investigative, operational, and collection material for more than one year. The FO must be notified when material stored in extended retention will be kept for additional time. A formal letter of request is not necessary. An e-mail is sufficient and should be placed in the case file to reflect the date of FO notification. The NCISRA shall provide the FO with copies of case control printouts to facilitate tracking and monitoring for delinquency unless the case control process is fully automated and FO personnel can print NCISRA case control reports. The NCISRA must establish a review system to ensure timely submission of disposition (DISP) sheet(s) for all cases closed with a disposition code "/F".

e. Submission to NCISHQ.

(1) Closed cases, with certain exceptions, will be forwarded directly to NCISHQ, RMB, Code 11C12. To ensure case integrity, an administrative quality control (QC) check must be completed before sending the case file to Code 11C12. Agent Notes are not forwarded to RMB unless specifically authorized/requested. Care must be taken to ensure the case file is complete. Verify that all documentation, including exhibits, attachments, and enclosures are properly labeled and marked (especially, security classification markings); and, all documents are in the proper order; and, the case file contains the current, properly completed, and signed RIMS coversheet and any other administrative documents as necessary. The 'Finished File' checklist, located on the NCISnet, Administrative website, Case Management Guidance, can be used to assist in this check. This checklist is a tool to assist reviewers with ensuring quality of case files, but is not required to be used or forwarded with the file.

(2) Cases with the following case categories will be sent directly to the cognizant operational code, NOT to RMB Code 11C12:

(a) DSI and SI cases are sent to the cognizant operational code.

(b) 5T and XXCT Cases are sent directly to NCISHQ Code 21B.

(c) 3C investigative/operational cases are sent directly to NCISHQ Code 22 (OSP).

(d) XXCE operations are sent directly to NCISHQ Code 22.

(e) Death (7H) cases are sent directly to NCISHQ Code 23B.

The operational codes are responsible for processing the completed case file and submitting it to RMB Code 11C12 upon its closure. They are responsible for adhering to all the administrative

procedures required of the FO except sending the e-mail described in subparagraph (4), below.

(3) Criminal/Law Enforcement case files (categories 4, 6, 7 and 8), not in the case categories cited in subparagraph (2), above, will be sent directly to RMB Code 11C12. It is the responsibility of the supervisory special agent of the sending office to ensure all existing documents are included in a closed case file and hard copies of child pornography are removed prior to the investigation being submitted to NCISHQ. In the event RMB is in receipt of closed case investigations prior to, or after June 2008, with questionable material attached, i.e., child pornography, the case file will be forwarded to NCIS Code 23 to conduct a technical review. If the material is found to contain contraband material, it will be returned to the field for corrective action per guidance in NCIS-3 Chapter 34, Sex Offenses. Upon receipt of case files, the RMB personnel will enter a "finished file" date in the Case Information System (CIS), which can be validated by FO/NCISRA review of CIS entries. Upon receipt of the cases identified in subparagraph (2), above, from the NCISHQ cognizant code, the Files Section will update CIS with a "finished file" date. This will officially establish that RMB received the case file. When a case in CIS has a finished file date of 02 August 2006, or forward, this may be accepted as proof that RMB Code 11C12 is in receipt of the case. No request for destruction approval/authority is required from RMB Code 11C12 for cases at the expiration of the one-year or extended retention period (see subparagraph 19-8.f. below). For cases in CIS with a finished file date prior to 02 August 2006, but not found in RIMS, forward a request for destruction authority directly to (b)(6) @NAVY.MIL.

(4) When preparing classified or unclassified CI/CT/CYBER case files for shipment to RMB, i.e., Categories 1, 3, 5, and 9, and not in the categories cited in subparagraph (2) above, send an e-mail with a list of the applicable case title and CCN to the "11C12 Files Section" at (b)(6) @NAVY.MIL; then, print a copy of the sent e-mail and include it in the package for shipment via U.S. Postal Service registered mail. This will facilitate to reference the original e-mail. Segregate classified from unclassified case files, and limit the number of files to less than 25 per shipment. This will make it easier for the Files Section to process the files and acknowledge receipt. Once the package is received and inventoried, Files Section personnel will enter "file receipt" information into the Case Management System (CMS) and reply to the original e-mail verifying receipt or non-receipt of individual case files. In the event of non-receipt, a copy of the case must be sent again to the Files Section with the current RIMS cover sheet per case. File Section's reply acknowledging receipt of the file serves as the official notification that the case file was received and, further, serves as the destruction authority for the case file once the one-year or extended retention period has expired. A copy of the e-mail should be placed in each case file at the field to document receipt. This precludes the need of sending RMB Code 11C12 a destruction request at the expiration of the one-year or extended retention period. As the cases identified in subparagraph (2), above, are sent to the NCISHQ cognizant code and not directly to Files Section, the FO must send a destruction request to (b)(6) @NAVY.MIL and receive approval to destroy the case file from Files Section. For files that were not received, Files Section will request another copy. Following the procedures previously cited, the acknowledgement of receipt sent by the Files Section will be the authority to destroy the copy in the field.

(5) Retained in FO: The following cases will be retained in the field and destroyed locally

at the end of their retention period. Destruction authority is not required from Code 11C12, but is granted by the provisions in SECNAV M-5210.1, Part III, under the applicable cited records series. Port Visit Support (5C) reports will be deleted from the database by the respective NCISHQ activity responsible for managing the database using this same disposition authority.

Records Series/ Case Category Code	**Record Series**	**Disposition Instructions**
CI/CT/Cyber		
Port Visit Support* 5C	3850.2a(1)	Destroy 25 years after case closure.
CI/CT Briefings 9E, 9M, 9S, 9T, 9Z	3850.2g	Destroy after 1 year or when no longer needed.
Threat Assessment (General) 5G	3850.2h	Destroy when superseded, obsolete, or no longer needed.
OPESEC Support Surveys (e.g., vulnerability assessments) 9E, 9M, 9S, 9T, 9Z	3850.2i	Destroy after next comparable survey (e.g., assessment), discontinuance of facility, or after 8 years, whichever is sooner.

* Per Gen Admin 21A-0065 dated 22 Oct 07, 5C Port Visit Support will be entered into the Port Visit Support database only. Force Protection Support (5C) cases will be sent to Code 11C12.

Records Series/ Case Category Code	**Record Series**	**Disposition Instructions**
Criminal		
Law Enforcement Briefings 9I, 9K, 9N, 9R, 9Z	5580.4d(3)	Destroy after 1 year or when no longer current, whichever is later.
STAAT		
Inspection Records 9Y	5520.1	Destroy after 3 years, upon conduct of the next comparable survey or inspection, or upon discontinuance of facility, whichever is later.

f. Destruction. The FO may destroy their file copies, to include 'agent notes' and other material (e.g., correspondence with original signatures, etc.), when:

(1) All investigative and disposition data has been entered into CLEOC for CRIM case categories 4, 6, 7, and 8, and all compliance reports indicate CLEOC completion.

(2) One-year retention or extended retention period for that file has expired. When any one of the following criteria is met, no additional approval is required from NCISHQ:

(a) Access RIMS to determine if the file is in RIMS. (RIMS contains all unclassified CI,

CT, CYBER, as well as law enforcement cases.) If so, open and view at least the cover sheet to ensure this is the same version that was submitted to RMB Code 11C12. Further review of the case file is encouraged to ensure that the imaged file is complete, but is not required.

(b) The FO is in receipt of a response e-mail from RMB Files Section that acknowledged the classified closed case file was received. These e-mail exchanges were as a result of when the FO mailed the classified original case file to RMB Code 11C12.

(c) Access CIS for CRIM case categories, as appropriate, to verify a "finished file" date on or after 2 August 2006. If the "finished file" date field is blank, or prior to 2 August 2006, NCISHQ destruction approval is required.

(3) For cases that do not meet at least one of the criteria cited above for destruction, the FO must forward a request for destruction authority to (b)(6) @NAVY.MIL. A response confirming that RMB is in possession of the file, is the authority to destroy the field copy of the case file. If RMB does not have the case file, a complete copy must be sent immediately with a current RIMS cover sheet attached.

19-8.2. USC Title 28, CFR, Criminal Justice Information System (CJIS) Security Policy and National Crime Information Center (NCIC) regulations require the logging of all criminal history (Interstate Identification Index (III)) requests. This function is performed at the NCISHQ switching computer and CyberLINXX server; however, NCIC regulations further require that any secondary dissemination of criminal history information be logged and that those logs be maintained for audit purposes. This log identifies the subject, date and recipient of all secondary disseminations of NCIS criminal history information outside of NCISHQ. The date within the CyberLINXX Criminal History Inquiry (QH) and or Menu Reason-For-Request (RFR) and clearly-identified Requestor's Name (RNM) fields maintained within the NCIS Information Technology Directorate (Code 15) system satisfies this requirement. The RFR will normally include the NCIS CCN or CLEOC IR number. A NCIC III criminal history record cannot be secondarily disseminated to the subject of the NCIC III record by a NCIS CyberLINXX server user. Neither NCIS Cyber LINXX server user(s) nor NCIS FO(s) are required to maintain a manual log book or NCIC III Secondary Dissemination hardcopy log provided the CyberLINXX user clearly records the RNM and RFR as part of the NCIC III QH and Criminal Record Request (QR) queries. The Department of Justice requires that the information contained in the log be maintained for one year. All categories of CI and criminal investigation files concerning persons entered into NCIC will be maintained in an open status by the control component for a minimum of six months or until the individual is located or cleared from NCIC, after which normal file retention and disposal criteria will apply.

APPENDIX (1): COUNTERINTELLIGENCE/COUNTERTERRORISM/ CYBER RECORDS

Case Category	SSIC (file number Series Title)	SSIC Number	Retention Period	Stored in RMB	Indexed in DCII
All category 3, 5, 9B[1], 9G[1], 9V 9X, and PCCIs.	Counterintelligence Investigations/Counter-intelligence Reports of a Routine Nature	3850, paragraph 2a(1)	25 years	Yes	Yes
Usually 3B, 3C, 3F, 3X, 5A, 5E, 5T, 9B[1], and 9G[1], and 9X.	Major CI/CT Investigations	3850, paragraph 2b(1)I2	50 years[2]	Yes	Yes
Case Category	**SSIC (file number Series Title)**	**SSIC Number**	**Retention Period**	**Stored in RMB**	**Indexed in DCII**
	Counterintelligence/Counter-terrorism Sources (FCI CW cases) (True Name)	3850, paragraph 2c	75 years	No[3]	No
	Counterintelligence/Counter-terrorism Special Operations (XXCE, XXCT)	3850, paragraph 2d(1)I2	50 years[2]	No	Yes
9F	CI/CT Defensive Briefings	3850, paragraph 2f	15 years[4]	Yes	Yes
9E, 9M, 9S, 9T, 9V, 9Z	CI/CT Briefings	3850, paragraph 2g	1 year	No[5]	No
5G	Threat Assessment (General)	3580, paragraph 2h	Destroyed when superseded, obsolete or no longer needed.	No[5]	No
5D, 9D, 5M	OPSEC Support Surveys	3850, paragraph 2i	3 years	No[5]	No
5S	CI/CT Studies	3850, paragraph 2j(1)	Delete when superseded or obsolete.	No[5]	No
1M	Foreign National Marriages	3850, paragraph 2k(1)	5 years	Yes	Yes
1K	Visa Applicants	3850, paragraph 2l(1)	5 years	Yes	Yes

9C, 9D	Technical Inspections and Surveys	3850, paragraph 2m	5 years	No[5]	No
1L and 1X	Local Security and Special Inquiries	3850, paragraph 2o	5 years	Yes	No
	Espionage Hotline Records (Information not referred)	3850, paragraph 2n(1)	2 years	No[5]	No
9A and 5V	Protective Operations[6]	5580, paragraph 4d(2)	5 years	Yes	Yes

Notes:

[1] 9B and 9G cases, conducted in support of an investigation, are treated as a part of the case file and indexed and filed under the Case Control Number (CCN).

[2] Files that meet the criteria as historical cases and have a permanent retention. At the conclusion of the retention period, RMB Records Center will coordinate with the NARA to arrange for their permanent transfer to NARA custody. Records that are classified under EO 12958, as amended, declassification review must be completed when the record is 25 years old from the date the case closed. RMB will coordinate declassification review with the DON Declassification Review contractor.

[3] These records are not currently stored in RMB Records Center, but will be at a future date.

[4] These records contain a consolidation of all like records pertaining to the subject. Retention dates begin from the date (i.e., year) of the most current material in the case file.

[5] These records are not retired to RMB Records Center, but are retained in and destroyed at the end of their retention period by the code with oversight of the specific case category.

[6] Protective Operation records were scheduled under law enforcement records in SSIC 5580, paragraph 4d(2). Persons named as subjects are indexed in the DCII.

APPENDIX (2): INSPECTION RECORDS

Case Category	SSIC (file number Series Title)	SSIC Number	Retention Period	Stored in RMB	Indexed in DCII
9Y	Military Security Survey and Inspection Program Records[1]	5522, paragraph 1	3 years[2]	No	No

Notes:
[1] These are STAAT inspection records.

[2] These records are retained by the originating office and are destroyed after three years, upon the conduct of next comparable survey or inspection, or upon discontinuance of facility, whichever is later.

APPENDIX (3): PERSONNEL INVESTIGATIVE RECORDS

Case Category	SSIC (file number Series Title)	SSIC Number	Retention Period	Stored in RMB	Indexed in DCII
2A	Agent Applicants for Positions with NCIS (not hired, but DoD-affiliated)	5527, paragraph 3a(1)(a)	5 years	Yes[1]	Yes
2A	Agent Applicants for Positions with NCIS (not hired and not DoD-affiliated)	5527, paragraph 3a(1)(b)	1 year	No[2]	No
2A	Agent Applicants for Positions with NCIS (hired)	5527, paragraph 3a(2)	10 years[1 & 3]	Yes	Yes
2B	Internal Inquires	5527, paragraph 3b	15 years[1]	Yes	Yes
2M	Limited Inquiries	5527, paragraph 3c	5 years[1]	Yes	Yes
2S	Support Applicants	5527, paragraph 3d	15 years[1]	Yes	Yes

Notes:

[1] These are Controlled Files. This means that the files are under special security within RMB Records Center and access to them is limited to those individuals specifically authorized access.

[2] These records are not retired to the RMB Records Center, but are retained and subsequently destroyed in NCIS Human Resource Directorate (Code 10) at the end of their retention period.

[3] Retention starts after release, separation, transfer, retirement, or resignation for the period specified in the above table before the file is destroyed or deleted.

APPENDIX (4): LAW ENFORCEMENT RECORDS

Case Category	SSIC (file number Series Title)	SSIC Number	Retention Period	Stored in RMB	Indexed in DCII
All 4, 6, and 7 (except 7H, and 7T), 9B[1] and 9G[1] closed prior to 1 January 1988 or offenses not on the DoD 5505.11 list. This includes USMC CID reports and reciprocal investigative files.	Criminal Investigative Reports Case files	5580, paragraph 4a(1)(a)	25 years	Yes	Yes
All 7H, 7T and 8 regardless of date. All 4, 6, 7, 9B[1] and 9G[1] closed on or after 1 January 1988 and are offenses on the DoD 5505.11 list. This includes USMC and Navy CID reports and reciprocal investigative files.	Controlled death and criminal sex investigations and investigations on or after 1 January 1988 where DoD 5505.11 requires offender criminal history	5580, paragraph 4a(1)(b)	50 years	Yes	Yes

All 4, 6, 7 and 8. This includes USMC and Navy CID reports. All crimes where no suspect is identified. (Exception: death and criminal sex cases will be filed under SSIC 5580, paragraph 4a(1)(b), above.)	Files determined to be of historical value based on widespread public interest, notoriety of the individual(s) and or the seriousness of the alleged offense(s)	5580, paragraph 4a(2)I2	50 years	Yes	Yes
	Topical files (Titled Under Name of Ship, Installation or Subject Code)	5580, paragraph 4b(1)(b)	5 years	Yes	No
	Case files	5580, paragraph 4b(1)(b)	25 years	Yes	No
	Weapons cases (This involves only cases that are Impersonal-Titles where a weapon with a known serial number is reported lost or stolen and is entered into the FBI automated National Crime Information Center (NCIC) index.)	5580, paragraph 4b(2)I2	5 years[2]	Yes	No
	Files from above determined to be of historical value based on widespread public interest, notoriety or the incident or the seriousness of the allegation				
This includes IRs and ICRs from Navy Law Enforcement and USMC Provost Marshal offices only. (USMC and Navy CID reports are filed under 5580, paragraph 4a(1)(b).	Incident Reports (IR)				
	Significant case files	5580, paragraph 4c(1)(a)	50 years	Yes	Yes
	Cases created prior to 1 January 1988	5580, paragraph 4c(1)(b)	25 years	Yes	Yes

Case Category	SSIC (file number Series Title)	SSIC Number	Retention Period	Stored in RMB	Indexed in DCII
	Non-Investigative Reports				
	Initiative operations – Group 1	5580, paragraph 4d(1)(a)	15 years	Yes	Yes
	Initiative operations – Group 2	5580, paragraph 4d(1)(b)	5 years	Yes	Yes
9A and 5V	Protective Operations	5580, paragraph 4d(2)	5 years	Yes	Yes[3]
This was covered under the 1st matrix for CI/CT***	Sources (for CRIM)	5580, paragraph 4d(4)	15 years	Yes	No
	Criminal Intelligence Reports) [4]	5580, paragraph 4d(5)	25 years	Yes	Yes4
	Fingerprint Card Files				
	Fingerprint card set 1 – Imaged version	5580, paragraph 11c(1)(a)	Send to FBI electronically	No	No
	Hardcopy fingerprint card	5580, paragraph 11c(1)(b)	Pending NARA approval	No	No
	Fingerprint card set 2	5580, paragraph 11c(2)	5 years[5] (Pending NARA approval)	No	No

Notes:

[1] 9B and 9G cases, conducted in support of an investigation, are treated as part of the case file and are indexed and filed under the Case Number (CN).

[2] Files that meet the criteria as historical cases and have a permanent retention. At the conclusion of the retention period, RMB Records Center will coordinate with the NARA to arrange for their permanent transfer to NARA custody. For records that are classified, the EO

12958, as amended, declassification review must be completed prior to 31 December of the 25th year from the year the case is closed. RMB Records Center will coordinate declassification review with the DON Declassification Review contractor.

[3] Protective Operation records were scheduled under law enforcement records in SSIC 5580, paragraph 4d(2). If there is a name of the person listed as the subject, that name is indexed in the DCII.

[4] CIR replaced the report titled "Report of Investigation (INFO)" which had replaced the title "NCIS Operational Reports (NORS)". They will remain ROI (INFO) for CI/CT/CYBER investigative reporting and will be filed under Counterintelligence Investigations/Counter-intelligence Reports of a Routine Nature, SSIC 3850.2a.

[5] Retained by Code 24 and destroyed at the end of their retention period.

APPENDIX (5): PERSONNEL SECURITY ADJUDICATION RECORDS

SSIC (file number Series Title)	SSIC Number	Retention Period	Stored in RMB	Indexed in DCII
Routine Actions	5529, paragraph 1a	15 years[1]	Yes	Yes
When affiliation with DoD is not completed	5529, paragraph 1b	1 year[2]	No	No
Adjudication decisions entered into electronic systems Reviews with no or minor issues that do not require documentation as addressed in SSIC 5529, paragraph 1a	5529, paragraph 1d(1)	1 year[2 & 3]	No	No
Reviews with issues	Use SSIC 5529, paragraphs 1a, 1b, 2a, or 2b, as appropriate	Use appropriate SSIC.	Yes	Yes
Contractor Case Review Records	5529, paragraph 1d(3)	1 year[2 & 4]	No	No
Significant Incidents or Adverse Actions	5529, paragraph 2a	25 years[1]	Yes	Yes
Precedent setting or wide spread public or Congressional interest	5529, paragraph 2b	25 years[5]	Yes	Yes

Notes:

[1] These records contain a consolidation of all like records pertaining to the subject. The retention date begins from the date (i.e., year) of the most current material in the case file.

[2] These files are retained and destroyed by the DON CAF.

[3] Destroy/delete after specified period of affiliation reflected in the above table.

[4] Destroy at the conclusion of their retention period and after verification that the case review record information is correctly entered into the Joint Personnel Adjudication System (JPAS) electronic system.

[5] These files are permanent and at the conclusion of the retention period, RMB will coordinate with NARA to arrange for their permanent transfer to NARA custody. EO 12958, as amended, requires completed declassification review of classified records in this category when the records are 25 years old from the date the case closed.

CHAPTER 20
TITLE: FREEDOM OF INFORMATION ACT POLICY
POC: 00LJF/FOIA
DATE: MAR 08

20-1. GENERAL

This chapter implements 5 USC 552, DOD Directive 5400.7 (series) and SECNAVINST 5720.42 (series) and sets forth-basic policy and procedures for making NCIS records available to the public.

20-2. POLICY

It is the policy of the NCIS to comply with the spirit and intent of the law in making records available to the public. A record exempt from public disclosure under the exemptions set forth in the Freedom of Information Act (FOIA) should nevertheless be made available to the public if no governmental interest would be jeopardized by the release of the record. If a record contains portions that are exempt as well as portions that are non-exempt, then any non-exempt portions that are "reasonably segregable" from exempt portions shall be released. Under no circumstances shall the withholding of a record be influenced by the possibility that its release might cause embarrassment or suggest error or inefficiency.

20-3. APPLICABILITY

20-3.1. The NCIS FOIA program is centrally administered and controlled at the NCISHQ. Field components of NCIS do not have either granting or denial authority for the release of records under the FOIA. Field components receiving written requests for release of NCIS records shall promptly refer such requests to NCIS Code 00LJF and so inform the requester. The outside envelope forwarding the request shall be prominently marked with the letters “FOIA.”

20-3.2. Members of the public making oral requests for NCIS records under the FOIA should be informed that all such requests must be submitted to Director, NCIS in writing. The request should reasonably describe the record(s) desired and indicate a willingness and ability to pay the costs associated with searching for and duplicating the record.

20-3.3. Naval commands may receive requests for copies of NCIS records in their custody. Commands are not authorized to release NCIS records and must refer the requests to the Director, NCIS along with a description or copy of the record held.

20-4. AUTHORITY

20-4.1. The Secretary of the Navy has delegated denial authority under the FOIA to the Director, NCIS. The Director has further delegated denial authority to the attorneys at NCIS Headquarters. . The Director has authorized the Information and Privacy Coordinator to release records requested under the FOIA, provided no part of the record is denied to the requester, and to sign routine FOIA matters, including referrals.

20-4.2. Personnel acting on FOIA matters in any way must have a detailed knowledge of this law and pertinent implementing directives. Copies of backup or explanatory material will be held by the Information and Privacy Coordinator and will be available for review.

20-4.3. The NCIS attorneys located at headquarters advise and act for the Director in matters relating to release of NCIS file information pursuant to the appropriate provisions of the FOIA, and supervise the operations of the staff assigned. It is the responsibility of the Information and Privacy Coordinator, NCIS Code 00LJF to ensure that time limits are met, that required records are maintained, and that changing interpretations of the law or changes to the pertinent directives are incorporated into NCIS policy.

20-5. FOIA REQUIREMENTS

20-5.1. To qualify as a request under the FOIA, a request for NCIS records must:

a. Be in writing, either in paper or electronic format

b. Reasonably describe the records desired, and

c. Contain payment of the anticipated fee or a statement that the requester is willing and able to pay such fees, or evidence that the requester is entitled to a waiver of fees.

20-5.2. Requests that are not “perfected” under the FOIA because they do not conform to the minimum requirements should nevertheless be answered promptly (within twenty (20) working days after receipt) in writing, in a manner calculated to assist the requesters in obtaining the desired records in accordance with the provisions of this chapter. For example, if such a request fails to contain a reasonable description of a desired record, the requester should be offered appropriate assistance in framing a new request in a way, which might facilitate identification of the record. If a

request fails to contain payment or a promise of payment of anticipated fees, information should be furnished upon which the requester may reasonably estimate the probable range of the fees that might be involved. Telephone contacts will frequently be useful for supplementing the required written communication.

20-5.3. In a case where a request is not "perfected" under the FOIA because of failure to include payment or a promise of payment of the applicable fees, but if the requested record is conveniently available and is releasable in its entirety, the Director NCIS may, if he determines that it will be in the best interests of NCIS to do so, provide a copy of such record in advance of payment or promise of payment of the applicable fees. The application of this provision shall be within the sole and exclusive discretion of the Director NCIS and shall not be construed as creating an exception to, or grounds for waiver of, the minimum requirements.

20-6. SCHEDULE OF FEES

The standard fees to be charged for the search and duplication of records are set forth in SECNAVINST 5720.42 (series). Personnel handling FOIA requests must be certain to record the computed costs for subsequent use in the annual report.

20-7. TIME LIMITS

20-7.1. Upon receipt of a proper FOIA request at NCIS, a determination to grant or deny the request must be transmitted to the requester within Twenty (20) working days of receipt of the request. The record must be made available, or a copy furnished the requester, promptly after a determination to release is made.

20-7.2. The twenty (20) day limit may be extended only by Director, NCIS and only if at least one of the following conditions prevails:

a. There is a need to search for records from activities separate and distinct from NCIS.

b. There is a need to search for, collect, and appropriately examine a voluminous amount of separate and distinct records requested in a single request.

c. The need for consultation with an activity outside the DON having a substantial interest in the determination or with a DON activity having a substantial subject matter interest in the request.

20-7.3. The extension of time shall include only that period of time reasonably necessary for proper processing of the request, but in no event may it exceed an additional 10 working days. If there appears to be a substantial possibility that the request might ultimately be denied, in whole or part, the Judge Advocate General, NCIS Code 14, shall be consulted prior authorization of the extension.

20-7.4. When properly authorized, an extension shall be effected by written notice to the requester prior to the expiration of the original time limit. The notice should state the reason for the extension and provide a date on which the determination can be expected.

20-8. EXEMPTIONS

20-8.1. Even though a determination can be made that governmental interest would be jeopardized by the release of the record, no matter may be withheld from disclosure to the public unless it falls within one of the following exemptions:

a. Matters specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign policy and are in fact properly classified pursuant to such Executive Order.

b. Matters relating solely to the internal personnel rules and practices of an agency.

c. Matters specifically exempted from disclosure by statute.

d. Trade secrets and commercial or financial information obtained from a person and privileged or confidential.

e. Inter-agency and intra-agency memoranda or letters that would not be available by law to a party other than an agency in litigation with the agency.

f. Personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of privacy.

g. Records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information.

(1) Could reasonably be expected to interfere with enforcement proceedings,

(2) Could deprive a person of a right to a fair trial or impartial adjudication,

(3) Could reasonably be expected to constitute an unwarranted invasion of personal privacy,

(4) Could reasonably be expected to disclose the identity of a confidential source, and in the case of a record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source.

(5) Would disclose law enforcement techniques and procedures,

(6) Could reasonably be expected to endanger the life or physical safety of any individual,

h. Contained in or related to examination, operating, or condition reports prepared by, on behalf of or for the use of an agency responsible for the regulation or supervision of financial institutions.

20-8.2. Geological and geophysical information and data, including maps, concerning wells.

20-8.3. Any reasonably segregable releasable portion of a record shall be provided to any person requesting such record after deletion of portions that are exempt from disclosure.

20-8.4. Exemption 7 is, of course, the exemption that will most frequently pertain to NCIS records. This exemption is explained in detail in section 20-17 of this chapter.

20-8.5. Security classification will play a part in the releasability of NCIS records. Whenever there is any question about the propriety of a security classification assigned to a requested record, the record will be referred to NCIS Code 22 for a determination whether the record's security classification marking is correct.

20-9. PROCEDURES

20-9.1. Upon receipt of a mailed FOIA request for a NCIS record, the Administration Department, NCIS Code 11C21, shall immediately route the request to the Information and Privacy Division, NCIS Code 00LJF.

20-9.2. The Information and Privacy Coordinator shall initiate whatever record keeping is required and take such action as is necessary to prepare a reply to the request. The Information and Privacy Coordinator shall maintain a concise record of the dates, parties and substance of all consultation with representatives of other activities or agencies and any communication with the requester. Requests shall be processed within twenty (20) working days in compliance with the provisions of the FOIA.

20-9.3. When the Information and Privacy Coordinator plans to recommend release of part of a record but to deny exempt portions that are "reasonably segregable," it is advisable to make such deletions from a reproduced copy of the record. The copy provided the requester should be a copy of the excised reproduction.

20-10. DENIALS

If it is determined that the requested records are exempt in whole or in part and that the exempt material should be withheld to protect the government's interest, the requester must be so notified. The notification must include the reason for the denial and the name and title of the person responsible for the denial. The notification shall also include specific citation of the exemption(s) upon which the denial is based, a brief discussion of the governmental interest protected by invoked exemption(s), and advisement that the requester has the right to appeal to the designee of the SECNAV (JAG or Office of the General Counsel (OGC) as appropriate), within 60 days. Additionally, if the denial is based in whole or part on a security classification, the notification shall include a summary of the particular provisions of DOD Regulations 5200.1 which contains the rationale for the correct classification of the record. The requester shall also be advised of his optional right to seek declassification review as an alternative to the right of appeal to the Secretary's designee.

20-11. OTHER AGENCY RECORDS

When a request is received which includes a record originated by an agency external to the DON, such request or part thereof shall be promptly referred to the originating agency and the requester so advised. In those situations in which the request is merely misdirected, referral to the proper agency will not require a response to the requester unless a "courtesy" response is indicated. The outer envelope used to refer a FOIA request to another agency shall be plainly marked with the letters "FOIA."

20-12. CONSULTATION

20-12.1. Consultation with other agencies having a substantial interest in the subject matter of the requested record(s) is required. Consultation with other offices and activities having substantial interest in or useful advice concerning the determination of requests is encouraged.

20-12.2. Consultation with the JAGor OCG is desirable when a denial of a request is expected to be appealed or judicially challenged. The Communications Directorate. NCIS Code 00C, must be consulted when the subject matter of a request is considered newsworthy, when a request is received from a news media representative, or when a denial is expected to be challenged publicly.

20-13. APPEALS

An appeal from an initial denial, in whole or in part, of a requested record must be in writing and be received by the appropriate official not more than 60 days following the date of transmittal of the notification of the initial denial. Except in situations where a brief extension is authorized, the appropriate official must make a final determination on an appeal within 20 days of receipt. Upon receipt, the appropriate appeal authority (JAG or OGC) shall notify the Chief of Naval Operations or Commandant of the Marine Corps, who will provide the file with such comments and recommendations as are appropriate. NCIS will be called upon to formulate a position on material it has denied. Personnel handling appeals shall give such matters HIGHEST PRIORITY.

20-14. ANNUAL REPORTS

The Information and Privacy Coordinator shall be responsible for preparation of the required report to the Office of the Chief of Naval Operations (N09B30) prior to 10 November of each year.

20-15. PENALTIES

The FOIA provides for sanctions of up to 60 days suspension against personnel who "arbitrarily and capriciously" deny members of the public legitimate access to records that should be released under the law.

20-16. INQUIRIES CONCERNING REQUESTERS PROHIBITED

Individuals who make requests under the FOIA will not be questioned concerning their motives, nor will any file checks, inquiries or investigations of any kind be conducted concerning requesters.

20-17. EXEMPTION 7 ANALYSIS

20-17.1. Exemption 7 pertains to those records or information compiled for "law enforcement purposes." The concept of "law enforcement" embraces criminal matters, civil actions to remedy or redress a violation of law, proceedings involving possible administrative sanctions and certain types of background investigation. Thus, with the exception of certain Category 9 cases, properly initiated NCIS investigations will be covered under the spectrum of "records or information compiled for law enforcement purposes."

20-17.2. Exemption 7(a) - Interference with enforcement proceedings. This basis for nondisclosure covers criminal, civil and administrative proceedings. It applies to matters, which are at the stage of litigation or adjudication. Investigations preliminary to adversary proceedings are protected.

20-17.3. Exemption 7(b) - Deprive a person of a fair trial or an impartial adjudication. This exemption is designed to protect the rights of private persons, including corporations and other organizations.

20-17.4. Exemption 7(c) - Unwarranted invasion of privacy.

20-17.5. Exemption 7(d) - Disclosure of confidential sources or information provided by such sources.

20-17.6. Exemption 7(e) - Disclosure of techniques and procedures.

20-17.7. Exemption 7(f) - Endangering the life of physical safety of any individual.

20-17.8. Implementation of Exemption 7 - Application of this provision of the law are frequently difficult and involve factors not foreseen beforehand. Each request must be processed on a case-by-case basis considering all applicable exemptions and whether governmental interest would be jeopardized by the release of the record.

20-17.9. Questions concerning FOIA matters should be addressed to the Information and Privacy Coordinator, NCIS Code 00LJF.

CHAPTER 21
TITLE: PERSONAL PRIVACY AND RIGHTS OF INDIVIDUALS (PRIVACY ACT)
POC: Code 00LJF
DATE: MAY 08

21-1. GENERAL

This Chapter implements 5 USC 552a, DoD Directive 5400.11 (series), SECNAV Instruction 5211.5 (series) and sets forth-basic policy and procedures concerning the rights of individuals to records concerning them as well as restrictions imposed on the collection and disclosure of personal information from records systems.

21-2. POLICY

21-2.1. It is the policy of NCIS to comply with the spirit and intent of the law in making personal records available to the subjects thereof. NCIS has published four record system notices, 1) DON CAF Personnel Security Adjudications Records, 2) FLETC NCIS Academy Records containing personal information pertaining to students and instructors, 3) records contained in the NCIS Investigative Files System and 4) records in the NCIS Administrative Files System. The Investigative and Administrative Files Systems are explained in detail at paragraphs 21-26 and 21-

21-2.2. The Secretary of the Navy (SECNAV), utilizing the authority granted to him/her in the Privacy Act of 1974, has exempted the NCIS Investigative Files System from various provisions of that law. However, it is the policy of NCIS, consistent with the provisions of the SECNAVINST, to exercise an exemption only when it would jeopardize governmental interest. All NCIS personnel are to be aware of, and abide by, the policy set forth below:

a. Preserve the personal privacy of individuals.

(1) Collect, maintain, use or disseminate any record of identifiable personal information only for a necessary and lawful purpose and in a manner which assures the information in such record is timely and accurate for the intended use.

(2) With certain exceptions, enumerated herein, permit an individual to know what records pertaining to him/her are collected, maintained, used or disseminated, and have access to and have a copy made, of all or any portions of such record and to correct or amend such records.

(3) Retain, in NCIS record systems, only such information about an individual as is reasonably necessary to accomplish the purpose or mission assigned to NCIS.

b. With respect to First Amendment rights, 5 USC 552a provides that no agency shall maintain any records describing how an individual exercises their guaranteed by the First Amendment including religious and political beliefs, freedom of speech and the press, and the right of assembly and to petition unless:

(1) Expressly authorized by statute or;

(2) Authorized by the individual about whom the record is maintained or;

(3) Within the scope of an authorized law enforcement activity.

c. No NCIS component will initiate any investigation or conduct an investigation at the request of competent authority when the predication of the investigation is mere expression of views and opposition to official U.S. policy. An investigation, within NCIS jurisdiction, may be initiated by a NCIS component or conducted at the request of competent authority only when one or more of the following elements is present:

(1) If the views being expressed are conjoined with the alleged commission of an act, which in itself would be a violation of a statute, regulation or directive. In such instances the alleged act would be the predication of the investigation.

(2) If the views are expressed in such a mode or manner as to indicate the possibility of sedition. It is to be noted that under the Uniform Code of Military Justice (UCMJ) and other federal statutes, sedition involves the acting in concert with another or others in opposition to lawful civil authority. Sedition is not present when an individual is acting alone.

(3) If the mode or manner of expression of views is in itself a violation of Article 88, UCMJ. Again, in such instances, the predication of the investigation shall be the alleged violation of the UCMJ.

(4) If an individual subject to the UCMJ, publicly utters statements or takes other actions with design to promote disloyalty or disaffection of such a nature as to constitute a violation of Article 134, UCMJ.

d. In the event of inability to reconcile the desires of a requesting command, with the above injunction, the matter shall be referred to the Director, NCIS for resolution.

21-3. RULES OF CONDUCT

21-3.1. Maintaining Personal Records. It is unlawful to maintain systems of records about individuals without prior announcement in the Federal Register. Anyone who does is subject to criminal penalties up to $5,000. Even with such notice, care shall be taken to keep only such personal information as is necessary to do what law, and the President, by Executive Order, require. The information is to be used only for the purpose described in the Federal Register. Only those systems of records described in the NCIS Investigative and NCIS Administrative Files System, or falling under the umbrella' of other Navy records systems, e.g., NCIS components are authorized to maintain personnel files. The information retained in those NCIS systems of records shall be used only for the purpose described therein.

21-3.2. Disclosure. Information about an individual shall not be disclosed to any unauthorized individual. Anyone who makes an unauthorized disclosure on purpose may be fined up to $5,000. Every member or employee of the DON who maintains records about individuals has an obligation to do their part in protecting personal information from unauthorized disclosure. SECNAVINST 5211.5E describes when disclosures are authorized.

21-3.3. Individual Access. Every individual, with certain exceptions, has the right to look at any record the DON keeps on them, to copy, and to request to have the record corrected if they consider it wrong. The individual attempting to exercise these rights shall be given courteous and considerate assistance.

21-3.4. Ensuring Accuracy. The DON has an obligation to use only accurate, timely, relevant, and complete information when making decisions about individuals. Every member, official, and employee involved in keeping records on individuals shall assist in the discharge of this obligation.

21-4. APPLICABILITY

21-4.1. This chapter governs the collection, maintenance, use and dissemination of personal information, and all requests from individuals who seek information on, access to, copies of, or amendments to records pertaining to themselves. All requests received from individuals for access to records pertaining to themselves, and which are located in an NCIS system of records, will be processed in accordance with this chapter, notwithstanding the fact that the requester may seek the record under the provisions of the Freedom of Information Act.

a. The NCIS Privacy Act Program shall be centrally administered and controlled at NCIS. Field components shall not have either granting or denial authority as it relates to notification, access or amendments of records within NCIS Investigative Files System. Special Agents in Charge (SAC) of the various NCIS field offices are authorized to grant, but not to deny, requests for notification, access and amendment as it relates to records within NCIS Administrative Files System. In responding to any such requests SAC are to be guided by this chapter. It should be noted that no exemptions have been established for records in NCIS Administrative Files System. Thus, no denials are authorized. Field components receiving written requests pursuant to the Privacy Act of 1974 for release of records within NCIS Investigative File System, shall promptly refer such requests to NCIS (Attn: NCIS Code 00LJF) and so inform the requester in writing. Privacy Act Requests may contain Privacy Protected Information and should be forwarded in a double wrapped envelope. The outside envelope shall be addressed to NCIS (Attn: NCIS-00LJF). The inside envelope forwarding the request to NCIS shall be prominently marked with the words PRIVACY ACT REQUEST.

b. Naval commands may receive requests for, or which include, copies of NCIS investigative records, which are in their custody at the time of the request. SECNAVINST 5211.5 series indicates that investigatory records compiled by an investigative organization remain the property of the originating investigative organization and must be destroyed or returned upon completion of official action. Insofar as it relates to requests for NCIS investigative material in their temporary custody, commands must refer such request to the Director, NCIS.

21-5. AUTHORITY/RESPONSIBILITY FOR DETERMINATION

21-5.1. SECNAV has delegated denial authority under the Privacy Act of 1974 to the Director, NCIS. The Director has further delegated the denial authority to a staff attorney, via the General Counsel NCIS Code 00L. This authority relates to records in NCIS Investigative Files System as well as to those in NCIS Administrative Files System. All requests submitted pursuant to the Privacy Act must be handled through the Information and Privacy Coordinator.

a. Responsibility for the coordination of all Privacy Act matters within NCIS shall rest with NCIS Information and Privacy Coordinator (NCIS Code 00LJF). Each NCIS field office SAC shall appoint a Privacy Coordinator. The functions of NCIS Field Office Privacy Coordinators include:

(1) Acting as the local point of contact for implementation and administration of the privacy program within their jurisdictional area.

(2) Insuring that the published NCIS systems of records describe those records retained by their subordinate offices, and that disclosure of personal information and accounting records are made in accordance with this chapter.

(3) Providing proper and continuing training of personnel connected in any way with records systems containing personal information. This is to be interpreted to mean all NCIS field office, NCIS Resident Agent and NCIS Resident Unit personnel.

b. The identity of the various NCIS Field Office Privacy Act Coordinators must be provided to NCIS Code 00LJF by January 15 of each year.

c. The Director, NCIS has been delegated authority to request records from a civil or criminal law enforcement activity under sub-section (b)(7) of 5 U.S.C. 552a. This authority has been further delegated to the SAC of NCIS field offices and Resident Agents in Charge of NCIS Resident Agencies. This chapter may serve as evidence of the above agents' authority to request such records. The above provision of the Privacy Act may be used when another federal agency has failed to include NCIS under its "routine use" description.

21-6. DEFINITIONS

21-6.1. The definitions set forth below are those, which are most important to the proper understanding of the Privacy Act of 1974.

a. Individual. Citizen of the United States or an alien lawfully admitted for permanent residence.

b. Record. Any item, collection or grouping of information, whatever the storage media (e.g., paper, electronic, digital, etc), about an individual that is maintained by or for the DON or any element thereof and which is retrieved by name or other personal identifier.

c. System of Records. A group of records under control of the DON or of any element thereof from which information is retrievable by the name of the individual or some other personal identifier.

d. Routine Use. Routine use means, with respect to the disclosure of a record, the use of such record for a purpose, which is compatible with the purpose for which it was collected. Routine uses for NCIS Investigative Files System and NCIS Administrative Files System are identified at paragraphs 21-26 and 21-27. Normally, this term is used in connection with inter-agency transfer of records rather than transfer within the Department of Defense (DoD) and the DON.

e. Disclosure. The conveyance of any information from a record by any method of communication to any other person or entity.

f. Notification. Refers to notifying an individual whether he/she is a subject of a record within a system of records.

g. Individual Access. Refers to access to a record by the individual or his/her designated agent or legal guardian.

h. Privacy Impact Assessment (PIA). An ongoing assessment to evaluate adequate practices in balancing privacy concerns with the security needs of an organization.

i. Protected Personal Information (PPI). Any information or characteristics that may be used to distinguish or trace an individual's identity, such as their name, social security number, or biometric records.

21-7. NOTIFICATION AND ACCESS PROCEDURES

21-7.1. SECNAV has exempted NCIS Investigative File System from the requirement to publish procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him/her, and with certain limitations, from the requirement to allow the individual to have access to those records within the record system which pertain to him/her. Individuals are not entitled to receive notification if a denial authority has exercised an exemption. While SECNAV has properly exempted NCIS from various provisions of the law, such exemption shall be exercised only if the record, or portion thereof falls under the exemptions specified in the Freedom of Information Act and disclosing the record would jeopardize governmental interest. Accordingly, all requests from an individual for notification/access to his records in the NCIS Investigative Files System shall be reviewed on a case-by-case basis and release determination made on the basis of the above policy. No exemptions exist for personal records contained in the NCIS Administrative Files System.

a. All requests under the Privacy Act relative to notification/accessibility of NCIS Investigative Files must be addressed to the Director, Naval Criminal Investigative Service, Code 00LJF, 716 Sicard Street, S.E., Suite 2000, Washington Navy Yard DC, 20388-5380. Requests must contain the full name of the individual and at least one additional personal identifier, such as date and place of birth or social security account number. Access to such investigative files will be limited to NCIS. Persons submitting written requests must properly establish their identity to the satisfaction of NCIS. Because of the sensitivity of the record involved, a signed statement or other certified form of identification might be required for all requests received by mail. Individuals appearing in person may present proof of identification in the form of military ID cards, valid driver's license or other suitable form of identification bearing a photograph and signature. Attorneys or other persons acting on behalf of a subject of a record must provide an authorization from the subject of the record, and that authorization must contain evidence that the subject of the record has provided an informed consent.

b. An individual's request for notification/access to their own record shall be granted if:

(1) The request is in writing and signed

(2) The request includes an unsworn declaration that states "I declare under perjury or penalty under the laws of the United States of America that the foregoing is true and correct and proper verification of identity is provided

(3) The system of records is adequately identified, and

(4) No exemption exists, or the exercise of an exemption is not warranted.

c. As previously indicated, even where an exemption exists, it would be exercised only when it would jeopardize governmental interest. Generally, the notification/access exemption will be exercised only if the requested material falls under the exemptions specified in the Freedom of Information Act (5 USC 552). Reasonably isolated portions of the records may be provided to the subject thereof after deletions of the portions falling within the above categories. The entire file may be withheld when it is properly exempted and exercise of the exemption is in the best interest of the DON.

d. If it is determined that denial of notification is proper, the requester shall be promptly advised via letter stating that no records from the NCIS Investigative Files System are available to him/her under the Privacy Act. The letter shall also inform the requester that administrative review of the decision may be sought within 60 days by letter to:

Office of the Judge Advocate General (Code 14)
1322 Patterson Avenue, S.E., Suite 300
Washington Navy Yard DC 20374-5066

The requester shall also be informed that any letter requesting such review should contain a copy of the letter of denial and his/her reasons for requesting the review.

e. If it is determined that denial of access is proper, the requester shall be sent a letter informing him/her of the denial. The letter shall include the reason(s) for the denial including citation of any applicable exemptions and a brief discussion of the significant and legitimate governmental purpose(s) served by the denial. The letter shall also inform the requester of the availability of an administrative review as specified in the preceding paragraph. If review of the requested records discloses that denial of access to portions of the record is proper, an expurgated copy of the record shall be provided to the requester with a denial letter in the manner and form discussed above.

f. An individual granted access to his/her record in person shall be required to provide written acknowledgement of such access. In instances where copies are provided as the result of requests, which are not made in person, the U.S. Postal registry record shall serve this acknowledgement purpose. If an individual is granted access to his records in person, a person of his own choosing to review the record may accompany the individual. The subject of a record shall be asked to furnish a written statement authorizing discussion of the record in the accompanying person's presence.

g. If copying is the only means whereby the record can be made available to the individual, e.g., when a copy must be made in order to delete information contained in the record pertaining to another individual, then reproduction fees shall not be assessed.

h. An individual shall be granted access to a medical record concerning him/her unless in the judgment of a physician access to such records could have an adverse affect upon the individual's physical or mental health. When it appears that release of that information to the individual could have an adverse affect on his physical or mental health, the medical record involved will be referred to the Bureau of Medicine and Surgery (BUMED) for opinion. When it has been determined by BUMED that access to medical records could have an adverse affect upon the

individual to whom it pertains, the individual may be asked to name a physician to whom the information shall then be transmitted. This shall not be deemed a denial of a request for access.

i. In those instances where requests for access to records is approved, acknowledgement to the requester shall be made within ten working days of receipt and access to the records provided within thirty working days.

j. Neither the law nor the implementing directives entitle an individual to have access to any information compiled in reasonable anticipation of a civil action or proceeding.

21-8. AMENDMENT/CORRECTION PROCEDURES

21-8.1. SECNAV has exempted the NCIS Investigative Files System from the provisions of the Privacy Act of 1974 relating to amendments. This exemption is to be exercised only when it would jeopardize governmental interest. When warranted, it may be exercised even though the individual was granted access to the records, i.e., the decision to grant access does not mean that a subsequent request for amendment must be approved. Notwithstanding the exemption, individuals who have been granted access to NCIS records pertaining to themselves may, and probably will, request that the record be amended. Such requests will only be considered if they are made in writing and addressed to the Director, NCIS Code 00LJF, 716 Sicard Street, S.E., Suite 2000, Washington Navy Yard DC 20388-5380.

a. The written request for amendment must include the following items:

(1) Description of the record. Requesters should specify the number of pages in the document(s), the title of the document(s), form numbers if there are any, dates and any other reasonable description, which identifies the document(s), in question.

(2) Description of the item to be amended. The description of the passages, pages, or documents should be as clear and specific as possible.

(3) Type of amendment. The requester must clearly state the type of amendment being requested.

(a) Expunge refers to a complete removal from the record of sentences, passages, paragraphs or documents.

(b) Correction refers to modification of the information in the record to make it more accurate, e.g., alter mistaken identities, dates, facts or other data pertaining to the individual.

(c) Other changes not representing deletions or corrections may be requested but they must be specifically and clearly described.

(4) Reason for Amendment. Each request for amendment must be based on specific reason, which must be identified in the request.

(5) Verification of identity. In order to assure that an individual's record is not accidentally or intentionally amended by an unauthorized person, all requests for amendments sent by mail must contain verification of identity of the requester. Individuals appearing in person must present satisfactory means of identity. (i.e., valid driver's license).

21-9. REVIEW OF REQUESTS FOR AMENDMENTS

21-9.1. Acknowledgement. A written acknowledgement of the receipt of a request for amendment of a record will be provided to the individual concerned within 10 working days, unless final action (approval or denial) can be accomplished within that time. In that case a notification of approval or denial will constitute adequate acknowledgement. If the request for amendment is presented in person, written acknowledgement may be provided at the time the request is presented.

21-9.2. Initial determination. In those instances where it is determined that the exercise of the exemption relative to amendment is not warranted, and the request is considered proper in all respects, the record shall be promptly amended and the requesting individual so notified. Individuals, agencies or components shown by accounting records to have received copies of the records or to whom disclosure has been made, will be notified of the approved amendments.

21-9.3. Where there is a determination to deny all or a portion of a request to amend a record, the following action will be taken:

a. Promptly advise the requesting individual of the basis for the refusal (i.e., authority) and the reason(s) therefore.

b. Inform the individual that he/she may request review of the matter within 60 days by addressing an appeal to:

(1) The Office of the Judge Advocate General (Code 14), 1322 Patterson Avenue, S.E., Suite 300, Washington Navy Yard, DC 20374-5066, if the matter concerns records other than performance evaluations.

(2) The Assistant Secretary of the Navy (Manpower and Reserve Affairs) Department of the Navy, 1000 Navy Pentagon, Washington, DC 20350-1000, if the matter concerns performance evaluations.

21-9.4. The appeal must be in writing and clearly state that it is a request for review of a refusal to amend a record made under the Privacy Act, and must either fully describe the circumstances of the request and initial denial, or attach a copy of the letter denying the request.

21-10. DENIAL DETERMINATION

The determination to deny a request to amend a NCIS record or any portion thereof, will be made only by the Director, NCIS or the officer acting for the Director. The Information and Privacy Coordinator, in submitting recommendations for the Director's consideration must bear in mind that investigative reports are largely a recitation of facts, report of actions taken and statements of

witnesses/sources. Errors relative to fact situations (e.g., wrong date of arrest, wrong charge, wrong person, etc.) should be amended upon presentation of evidence of inaccuracy. On the other hand, statements of witnesses/sources are occasionally inaccurate. Nevertheless, the security of those statements must be preserved as changes could destroy the integrity of the investigative process. This information is generally relevant and necessary to accomplish a purpose or function required to be performed by the DON pursuant to a statute or Executive Order. Firm and specific guidance for granting amendments to records in the NCIS Investigative Files System is neither possible nor desirable. Each request must be judged on its own merits giving full consideration to the variety of factors involved.

21-11. DISCLOSURE

21-11.1. No record contained in a system of records shall be disclosed except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless disclosure of the record falls within one of the areas noted below. Disclosures to third parties on the basis of a written consent or request of the individual concerned is permitted, but not required. The disclosure provisions pertain to both the NCIS investigative and administrative record systems.

a. Disclosure may be made to those officials and employees of the DoD or DON who have a need for the record in the performance of their duties when the use is compatible with the purpose for which the record is maintained. This disclosure provision would include dissemination to naval commands, DON personnel managers, DON medical offices, etc., as well as to those personnel or elements of the DoD, which might have similar need for the record. Note: No disclosure accounting required.

b. Disclosure may be made as required by the Freedom of Information Act. Note: No disclosure accounting required.

c. Disclosure may be made for a routine use as defined in Chapter 21-paragraph 6.1.d. above and as described in the NCIS Record Systems notices. Note: Disclosure accounting is required.

d. Disclosure may be made to the U.S. Census Bureau for purposes of planning and carrying out census or survey or related activity authorized by law. Note: Disclosure accounting is required.

e. Disclosures may be made to a recipient who has provided adequate written assurance that the record will be used solely as a statistical research and reporting record provided the record is transferred in a form that is not individually identifiable. Note: Disclosure accounting is required.

f. Records may be disclosed to NARA as a record that has sufficient historical or other value to warrant its continued preservation by the U.S. Government, or for evaluation by the Archivist of the United States or his designee to determine whether the records has such value. Note: Disclosure accounting is required, unless the records are permanently transferred to NARA without NARA's prior review of the actual material.

g. Disclosure may be made upon the written request of the head of an agency outside of DoD or his delegate for a civil or criminal law enforcement activity when the request specifies the particular record desired and the law enforcement purpose for which the record is sought. Disclosure under this provision may be made whether or not a routine use (21-11.1.c above) has been established for the intended disclosure. The agency seeking disclosure may ask for disclosure under this provision rather than under routine use for reasons of its own including a desire to protect the disclosure accounting record from access by the individual of record. Blanket requests for all records pertaining to an individual shall not be honored. Disclosure to foreign law enforcement agencies is not covered under this provision. Such disclosures may be made only pursuant to the routine use described in the NCIS Record Systems Notice. Note: Disclosure accounting is required.

h. Disclosure may be made under emergency conditions involving compelling circumstances affecting the health and safety of a person. The individual about whom the records are disclosed need not necessarily be the individual whose health or safety is in peril. Note: Disclosure accounting is required.

i. Disclosures may be made to either House of the United States Congress or, to the extent of matters within its jurisdiction, to any committee or sub-committee thereof or to any joint committee of Congress or sub-committee thereof. Release to members of Congress acting in their individual capacities or on behalf of their constituents shall be processed in accordance with the provisions of the routine use' provision promulgated by DON. Note: Disclosure accounting is required.

j. Disclosure may be made to the Comptroller General of the United States or to any of his authorized representatives. Note: Disclosure accounting is required.

k. Disclosure may be made in response to an order from a court of competent jurisdiction. Individuals handling requests of this nature are enjoined to follow the guidance provided in the SECNAV Instruction. Note: Disclosure accounting is required.

(l) Disclosure to a consumer reporting agency in accordance with the Debt Collection Act, 5 U.S.C. § 552a(b)(12). Note: Disclosure accounting is required.

21-11.2. Personally identifiable information should not be disclosed. Lists of names and other personally identifying information (to include lists of e-mail addresses) of personnel currently or recently assigned within a particular component, unit, organization, or office within the DoD should not be disclosed. This includes active duty military personnel, civilian employees, contractors, member of the National Guard and Reserves, military dependents, and Coast Guard personnel when the Coast Guard is operating as a service in the Navy.

21-11.3. Records of juveniles require special handling pursuant to the juvenile delinquency act (18 USC 5038) as amended 1984. Appropriate safeguards are required in handling and disseminating these records.

21-12. ACCOUNTING FOR DISCLOSURE

21-12.1. The purpose of the accounting requirement is:

a. Allow individuals to determine to whom their records have been disclosed.

b. Provide a basis for subsequently advising recipients of records of any dispute or corrected records.

c. Provide an audit trail for subsequent review of activity compliance.

21-12.2. Except for disclosures made to personnel of the DoD and DON in connection with their routine duties, and disclosures required by the Freedom of Information Act, it is mandatory that an accounting be kept of all disclosures of personal records from an NCIS record system. It is the responsibility of the individual making the disclosure to ensure that proper accounting records are prepared.

21-12.3. Contents of disclosure record. The disclosure record must contain the date (year, month, and day), nature and purpose of disclosure and the name and address of the person and agency to whom the disclosure is made. The record of accounting must be retained for least five (5) years after the last disclosure, or the life of the record, whichever is longer.

21-12.4. The accounting for disclosure is to be made at the time of disclosure utilizing OPNAV form 5211/9 Disclosure Accounting Form, or in the Report of Investigation (ROI), etc. Since accounting for disclosure pertains only to the disclosures of personal information indexed (name and identifying data) into the NCIS retrieval system relating to U.S. citizens and aliens legally admitted for permanent residence, reports not containing personal information on non-indexed individuals, as well as those relating to foreign nationals, do not require any disclosure accountability. Even though the "copy to" formatting entries on a document might be interpreted as establishing disclosure, completion of the Disclosure Accounting Data is nevertheless required. A disclosure accounting is also required when providing personal information on individuals to a crime laboratory outside of DoD along with evidence for examination. Generic title reports should not require disclosure accounting since witnesses named therein would not normally be cross-referenced into a system of records.

21-12.5. Field personnel making authorized disclosures of investigative records outside of DoD will more frequently than not be making them under the “Routine Use” provisions of the law. When disclosures are made while an investigation is in its pendency, the required disclosure data will be entered on the ROI, etc., from which the disclosure is made. This will be a separate caption in the last paragraph of the narrative in the ROI and will appear as the caption “DISCLOSURE ACCOUNTING.” The disclosure accounting paragraph must contain the date (year, month and day), nature and purpose of disclosure and the name and address of the person and agency to whom the disclosure is made. When authorized disclosures are made outside of DoD after completion of an investigation, and the closing report has already been submitted to NCIS, OPNAV form 5211/9 Disclosure Accounting Form, will be utilized and forwarded directly to NCIS Code 11C1. It is possible that disclosure will be made outside of DoD even though NCIS does not have either a pending or completed case. Where warranted, a case should be opened and

the Disclosure Accounting reflected on the opening document. When the opening of a case cannot be justified, OPNAV form 5211/9 Disclosure Accounting Form, should be completed and forwarded to NCIS along with an explanation of the disclosure, providing the disclosure is made from records in a NCIS system of records. In those instances where the Disclosure Accounting Sheets are sent directly to NCIS Code 11C1, it will be essential that full identifying data be included on the accounting sheets. These accounting sheets are to be forwarded in envelopes the outside of which are prominently marked, "Privacy Act Disclosure Accounting Record." When the opening of a case cannot be justified, and where the information has been obtained from a non-NCIS records system (e.g., command personnel) to satisfy a legitimate request, a disclosure accounting must be entered with the record in the system from which obtained. While NCIS personnel have no disclosure accounting responsibility in such instances, in the spirit of complying with the Act there rests an obligation to inform non-NCIS records custodians of the records' intended use outside of DoD and of the custodians' disclosure accounting responsibility. When another agency requests record information under the provisions of Section (b)(7) of the Privacy Act for law enforcement purposes, and further requests an exception under Section (c)(3) from release of its identity to the individual, a NCIS document (ROI) must be prepared noting the exception and forwarded to NCIS. Accounting records for the disclosure of records in the NCIS Administrative Files System will be retained at NCIS.

21-12.6. Personnel in operational divisions at NCIS may also, on occasion, disclose personal records from an NCIS record system to a non-DoD source. It will be incumbent upon the individual making the disclosure to prepare a disclosure accounting sheet. For investigative records, if the individual making the disclosure is in possession of a dossier, the Disclosure Accounting Sheet should be placed on the left hand side thereof. If the dossier is not available to the individual, the Disclosure Accounting Sheet should be provided to NCIS Code 11C1 for proper filing. Disclosure Accounting Sheets pertaining to disclosures of records from the NCIS Administrative Files System will be retained with the file involved, if one exists. If not, NCIS Code 11C1 will retain the accounting sheet in an alphabetical file separated from all other files.

21-12.7. Liaison Section of the Records Management Branch (NCIS Code 11C11) is responsible for, among other things, releasing of files to representatives of other agencies accredited for that purpose. Such disclosures may continue as such usage has been provided for under the "routine use" description of the NCIS Investigative Files System notice in the Federal Register. Personnel of this Branch must bear in mind that the "routine use" provision allows release only when the purpose is compatible with the purpose for which the record is maintained. Questions relating to the propriety of any particular disclosure should be brought to the attention of NCIS Code 00LJF. NCIS Code 11C11 shall ensure that Disclosure Accounting Sheets are prepared for all of its disclosures to non-DoD agencies.

21-12.8. Upon request from an individual for records about him or herself, NCIS Code 00LJF shall include accountings for disclosure for release processing. With two exceptions, all information in the accountings for disclosure will be released to the individual. An accounting for disclosures documenting the release for records based upon the written request of the head of another agency or government instrumentality for law enforcement purposes will not be reported to the individual requester (5 USC 552a(b)(7)). An accounting for disclosures documenting the release of records to a court of competent jurisdiction in those situations when the order of the

court is not a matter of public record will not be reported to the individual requester (5 USC 552a(b)(11)). To preclude inadvertent disclosures in these two areas, a copy of the written request or a copy of the face sheet of the court order shall be appended to the Disclosure Accounting Sheet.

21-12.9. Disclosure of DCII tracings. As a general rule, DCII tracings are not to be disclosed to personnel employed outside of the DoD. In those rare instances when such disclosure is necessary, it will be incumbent upon the individual making the disclosure to complete a Disclosure Accounting Sheet. That sheet will be provided directly to the Head, Records Management Division, NCIS Code 11C1. In order to centralize the DCII disclosure accounting system, the latter individual will provide the Defense Security Service (DSS) with a copy of the DCII terminal printout annotated to meet the requirements of the Privacy Act. The accounting sheet shall be retained for 30 days and then destroyed.

21-13. EXEMPTIONS

21-13.1. General exemptions Subsection (j)(2) of the Privacy Act of 1974 authorizes agency heads to exempt a system of records from certain provisions of the law if that system of records is maintained by a component which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, corrections, probations, pardons or parole authorities and which consist of:

a. Information compiled for the purpose of identifying individual criminal offenders and alleged offenders consisting only of identifying data, notations of arrest, the nature and disposition of criminal charges, sentencing, confinement, release and parole and probation status.

b. Information compiled for the purpose of a criminal investigation including reports of informants and investigators and associated with an identifiable individual.

c. Reports identifiable to an individual compiled at any stage of the process of enforcement of criminal laws from arrest or indictment through release from custody.

21-13.2. Specific exemptions. Section (k) of the Privacy Act authorizes agency heads to promulgate rules exempting any system of records within the agencies from certain subsections of the Privacy Act if the system of records is:

a. Subject to the provisions of Section 552(b)(1) of the Freedom of Information Act. This Section, identified under the Privacy Act as 552a(k)(1), pertains to matters specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign policy and are in fact properly classified pursuant to such Executive Order. NCIS Investigative File System has been authorized this exemption.

b. Investigative records compiled for law enforcement purposes other than those criminal investigative records covered under a general exemption ((j)(2), above). Records of this type relate to non-criminal (exclusive of PSI) investigative matters of which categories 3X and 5X investigations are sometime examples. DoD ruled in 1980 that criminal law enforcement agencies

authorized the (j)(2) exemption no longer will be permitted a separate exemption for non-criminal (exclusive of PSI) investigative matters as provided under 5 U.S.C. 552a(k)(2). As a primarily criminal law enforcement agency with the general (j)(2) exemption, NCIS may continue to maintain records on non-criminal matters despite no longer holding the specific (k)(2) exemption for its Investigative Files System. An individual shall be provided access to non-criminal investigative matters that have been used to deny him/her a right, privilege, or benefit unless such access would reveal a NCIS Asset. Paragraph 21-14.3.a. also relates.

c. Records maintained in connection with providing protective services to the President of the United States or other individuals authorized such protection. The NCIS Investigative Files System has been authorized this exemption (5 U.S.C. 552a(k)(3)).

d. Records used only for statistical research or other evaluation purpose. The NCIS Investigative Files System has been authorized this exemption (5 U.S.C. 552a(k)(4)).

e. Investigative records compiled solely for the purpose of determining suitability, eligibility, or qualifications for federal civilian employment, military service, federal contracts, or access to classified information, but only to the extent that providing an individual with access to such records could reveal the identity of a confidential source. Categories 1 and 2A records at NCIS fall under this exemption. The NCIS Investigative Files System has been authorized this exemption (5 U.S.C. 552a(k)(5)). The exemption applying in Category 2B matters will vary depending upon whether the orientation is criminal ((j)(2)) or personnel ((k)(5)) in nature.

f. Test or examination material used solely to determine individual qualifications for appointment or promotion in the federal service, the disclosure of which would compromise the objectivity or fairness of the testing or examination process. NCIS has been authorized this exemption (5 U.S.C. 552a(k)(6)).

g. Evaluation records used for determining potential for promotion in the armed services, but only to the extent that providing an individual with access to such records would reveal the identity of a confidential source. NCIS has not been authorized the use of this exemption (5 U.S.C. 552a(k)(7)).

21-13.3. SECNAV has promulgated rules exempting the NCIS Investigative Files System from appropriate provisions of the Privacy Act under both the General and Specific exemptions. As indicated previously, it is the policy of NCIS to exercise an exemption only when it serves a significant legitimate governmental purpose. Each case will be considered on its own merits.

21-14. CONFIDENTIALITY

21-14.1. The Privacy Act differentiates between an implied and an expressed promise of confidentiality, with the definitions being as indicated below:

a. Express promise: a specific promise to a source that his/her identity will be held in confidence.

b. Implied promise: interviews of sources prior to 27 September 1975 under circumstances from which the source could reasonably infer a promise of confidentiality.

21-14.2. Sources from whom information is solicited for law enforcement purposes, other than criminal activities, must be advised that under the provisions of the Privacy Act their identities may be disclosed to the individual to whom the record pertains, upon request, unless the source expressly requests that his or her identity not be revealed as a condition of furnishing the information. Such pledges of confidentiality are to be limited to the most compelling circumstances. The Office of Management and Budget (OMB) guidelines suggest the following circumstances as warranting a pledge of confidentiality:

a. Without the information thus obtained, unacceptable, untrustworthy or incompetent persons might be selected.

b. The potential source would be unwilling to provide needed information without a guarantee that his identity will not be revealed to the subject.

c. To be of value in the personnel screening and often highly competitive assessments in which it will be used, the information must be of such a degree of frankness that it can only be obtained under an express promise that the identity of its source will not be revealed.

21-14.3. It seems obvious from the above that pledges of confidentiality may not be given routinely. Generally, such pledges are not warranted for non-derogatory information unless that information is considered essential to a proper determination. Agent applicant pre-employment inquiries clearly fall within paragraph 21-14.2.c. above and agents should not be hesitant to extend a pledge of confidentiality when such appears necessary to achieve the degree of frankness required. This should not, however, be viewed as authorization for blanket use of confidentiality in such investigations.

21-14.4. If an investigation is initiated to determine if a violation of the UCMJ or the U.S. Code has occurred, that case is considered a criminal investigation for purpose of the Privacy Act. Accordingly, SECNAV exempts them from certain provisions of that Act. Therefore, neither Privacy Act statements nor pledges of confidentiality need be afforded in those cases initiated to determine criminal activity.

a. The issues may be framed in terms of criminal reference in virtually all investigations conducted by NCIS. By so doing, the use of Privacy Act Statements and pledges of confidentiality is not required. A few investigations, particularly Categories 3X and 5X, where inquiries may be conducted to determine non-criminal (suitability) issues, require that Privacy Act Statements be afforded to subjects, if interviewed, and pledges of confidentiality considered when interviewing sources. Where doubt as to criminal involvement exists, it is better to weigh in favor of affording pledges of confidentiality to sources to assure their protection if the subject accesses his file under the Privacy Act. If an investigative report cannot be defended as an inquiry involving criminal activity, the identity of sources can only be withheld under provisions of the Privacy Act where express promises of confidentiality have been given. NCIS Code 22A should be consulted on operational aspects in these investigative matters, and NCIS Code 00LJF on Privacy aspects.

21-14.5. Normally, the source will be given the confidentiality advisement after the agent has identified himself/herself and stated the purpose of the investigation. If the source expresses a desire for confidentiality, the agent should then explain that such pledges could only be given if the information held falls within the categories noted in paragraph 21-14.2.a. through c. or is otherwise considered germane to the investigation. If the source indicates that the information held does meet the confidentiality criteria, the agent may assure the source that his identity will be protected. If the source indicates that the information held is of a routine, favorable nature, the agent will have to decide whether it warrants a pledge of confidentiality under the particular circumstances of the case or if the information should be sought from other sources. When a pledge of confidentiality is given the source shall be listed in the report as a NCIS asset.

21-14.6. Privacy Act requirements for the conduct of record checks such as employment, education, local agency check, etc. are basically the same as set forth above. The record custodian or official of the firm or local non-federal agency must be informed that its identity may be disclosed to the individual concerned upon a request from that person. Express promises of confidentiality may be given when the custodian or official indicates that the information will be provided only if the identity of the firm/agency is protected. Information held by employers, schools, etc. is essential to the completion of various law enforcement investigations. Thus, pledges of confidentiality may be given even where the information is not derogatory or adverse. Such pledges shall, however, be given only when required to get the needed information. In situations in which field components have continuing contact with a firm or agency, it will be satisfactory to provide the Privacy Act advisement on a periodic basis, but not less than twice a year.

a. Several foreign governments, the United Kingdom in particular, have either conducted personnel security investigations on behalf of DoD or have furnished information for inclusion in Background Investigations. They have expressed concern regarding the protection of the information furnished under provisions of the Freedom of Information Act (5 USC 552) and the Privacy Act of 1974 (5 USC 552a). Many of these governments desire that their identities be protected and that none of the information they furnish be released either to the subject or the public.

(1) Neither of the above statutes is necessarily a bar to denying the subject of an investigation or the general public access to material derived from foreign sources in those instances in which the data is classified by a foreign government or when the material has been released to a DoD agency under a pledge of confidentiality to the foreign government.

(2) Executive Order 13292, Section 1.6(5)(e), explicitly provides that:

“Foreign government information shall retain its original classification markings or should be assigned a United States classification that provides a degree of protection at least equivalent to that required by the entity that furnished the information.”

(3) Executive Order 13292, Section 6.1(r), explicitly provides that Foreign government information means:

(a) Information provided to the United States Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation, that the information, the source of the information, or both, are to be held in confidence; or

(b) Information produced by the United States pursuant to or as a result of a joint arrangement with a foreign government or governments or an international organization of governments, or any element thereof, requiring that the information, the arrangement, or both, are to be held in confidence.

(4) This is consistent with the amended Freedom of Information Act, 5 USC 552 which expressly exempts from public disclosure material that is authorized to be kept Secret under criteria established by an executive order (E.O. 12958). Section (k)(1) of the Privacy Act of 1974 also recognizes the need for protecting classified material.

(5) Therefore, if a foreign government does not wish to be identified as a source or reveal the information provided, it must either classify the information it shares with NCIS or provide the information only under an express pledge of confidentiality.

b. Criminal justice record material compiled for the DSS is not collected to be used in connection with the enforcement of criminal laws, but solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service or access to classified information. Under the law, the DSS can honor pledges of confidentiality made to a foreign government or simple pledges to protect the information it has furnished.

c. Overseas components should assure their foreign counterparts that investigative data furnished to the DoD could and will be protected, when it is either classified by the foreign source or provided under a pledge of confidentiality. In either case, the material will be given a U.S. classification, where appropriate, and protected to the same degree practiced by the foreign government or international organization.

21-14.7. Agents must bear in mind both when granting pledges of confidentiality in non-criminal cases, and in writing their reports, that if information from a confidential source is used to deny an individual a right, benefit or privilege, it may be necessary at least to summarize the information if the individual should request it on the basis of such a denial.

21-14.8. In those instances where Privacy Act Statements and/or Privacy Act advisements are required, the NCIS documentation reporting the interviews must contain information confirming compliance with such requirements. Due to the variety of documents, which may be involved, flexibility in this reporting is required. Normally, the paragraph reporting the interview of the person to whom the record will pertain (usually the subject) should include a simple statement that a Privacy Act Statement was given. In the case of interviews of third parties, the paragraph reporting results of the interviews may vary. (b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(b)(7)(E) If numerous third party interviews are reported in the same document, one separate paragraph, at or near the end of the document, may simply state that all interviewees were provided a Privacy Act advisement and none desired confidentiality. Or conversely, it may state that all interviewees were provided a Privacy Act Advisement and that only the person(s) whose interview is reported in identified paragraph(s) desired confidentiality.

21-15. CLASSIFIED RECORDS

Subsection (k)(1) of the Privacy Act exempts records specifically authorized under criteria established under an Executive Order to be kept Secret (i.e., classified) in the interest of national defense or foreign policy and are in fact properly classified pursuant to such Executive Order. In those instances where NCIS has jurisdiction over classified records involved in a request for notification, access or amendment, those records must be subjected to a security determination and the security clearance of the requesting individual must be determined before an exemption is exercised and a request denied. In those situations where NCIS lacks classification jurisdiction over the classified portions of the requested records, immediate coordination shall be established with the official/activity having classification jurisdiction.

21-16. PRIVACY ACT STATEMENT

21-16.1. Subsection (e)(3) of the Privacy Act requires that individuals from whom personal information is requested for a system of records be informed of:

a. The authority (statute or Executive Order), which authorizes the solicitation. (Where no specific statute or Executive Order exists 5 U.S.C. 301 may be cited.)

b. All major purposes for which the Department of Defense uses the information, e.g., suitability for employment, eligibility for entry into the U.S., retention in the Armed Forces, etc.

c. A brief summary of those “routine uses” to be made of the information as published in the Federal Register.

d. Whether disclosure is mandatory or voluntary and the possible consequences for failing to respond.

21-16.2. The Privacy Act Statement must be given regardless of the medium used in requesting the information. When the information is collected in an interview, the interviewer should orally summarize the above information before the interview begins and provide the individual with a statement that can be retained.

21-16.3. SECNAV has exempted the NCIS Investigative Files System from the above requirements to the extent that the action involves the enforcement of criminal laws. Accordingly, there is no requirement to provide the Privacy Act Statement in any NCIS activity pertaining to criminal matters. It is, however, required for all other types of investigations, as well as screening board interviews, pre-employment inquiries involving subject interviews, background

investigations involving Subject interviews conducted on behalf of the DSS, and requests for personal information to support the Personnel Management System

21-17. SOCIAL SECURITY NUMBER

21.17.1. An individual may not be denied any right, privilege or benefit provided by law as the result of refusal to disclose his Social Security Number (SSN), unless such disclosure is required by statute or, in the case of systems of records in existence and operating before 1 January 1975, where such disclosure was required by statute or regulation prior to 1 January 1975.

21.17.2. When an individual is requested to disclose their SSN, they must be informed:

a. Whether such disclosure is mandatory or voluntary.

b. By what statute or other authority the number is solicited.

c. What uses will be made of it.

21-17.3. Once a military member or civilian employee of the DON discloses their SSN for purposes of establishing personnel, financial, or medical records upon entry into naval service or employment, it is not required that such individual be informed as noted above when they are subsequently requested to provide or verify this identification number. As a general rule, then, NCIS personnel requesting an individual to provide a SSN will only have to do so when that individual is not a member or employee of the DON.

21-18. FEES

Individuals may request copies of any NCIS document concerning them to which they are granted access. They will be charged only for the reproduction of such documents. However, when an individual cannot reasonably appear in person for access to personal records or where it is necessary to reproduce copies in order to excise certain information no reproduction charge will be assessed. No search fee is authorized.

21-19. TRAINING

The Privacy Act requires that all personnel whose duties involve responsibilities for the design, development, maintenance, custody and use of systems of records affected by the Privacy Act be educated and trained relative to its provisions. As a matter of policy, all NCIS personnel are to receive indoctrination relative to the provisions of the Privacy Act. The NCIS Information and Privacy Coordinator (NCIS Code 00LJF) shall be responsible for ensuring that proper indoctrination is effected and that such training includes newly hired personnel.

21-20. NEW SYSTEMS OF RECORDS

No new systems of records will be created without the specific approval of the Director, NCIS. Approval of any such requests will be granted only after compliance with the requirements of the

Privacy Act. All additions to the Category of Records described in the NCIS Records Systems Notices will be reported to the NCIS Information and Privacy Coordinator.

21-21. RELEASES TO A SUBJECT OR DEFENSE COUNSEL

21-21.1. Previous paragraphs set forth policy and procedures for release of record information under the provisions of the Privacy Act. In addition to the requirements of the Privacy Act, it is NCIS policy to release certain investigative record information to Subjects of recent investigations or counsel acting on their behalf.

21-21.2. Recognizing that the parties in an NCIS investigation may have a legitimate interest in having timely access to the results of the completed investigation, it is NCIS policy to make those reports available to Subjects of investigation, or counsel acting on their behalf, in cases where Command administrative or disciplinary action is contemplated, and where no governmental interest would be jeopardized by withholding the reports. In this context, reports of investigation in closed criminal cases will generally be releasable, including results of polygraph examinations. Actual polygraph charts and associated testing and evaluation worksheets, however, are not releasable.

a. Reports made available to subjects and their counsel are subject to the exemptions of Freedom of Information Act. Exemptions are:

(1) Matters specifically authorized under criteria established by an Executive Order to be kept Secret in the interest of national defense or foreign policy and are in fact properly classified pursuant to such Executive Order.

(2) Matters relating solely to the internal personnel rules and practices of an agency.

(3) Matters specifically exempted from disclosure by statute.

(4) Trade secrets and commercial or financial information obtained from a person and privileged or confidential.

(5) Inter-agency and intra-agency memoranda or letters which would not be available by law to a party other than an agency in litigation with the agency.

(6) Personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of privacy.

(7) Records compiled for law enforcement purposes, but only to the extent that the production of records would:

(a) Interfere with enforcement proceedings,

(b) Deprive a person of a right to a fair trial or impartial adjudication,

(c) Constitute an unwarranted invasion of personal privacy,

(d) Disclose the identity of a confidential source, and in the case of records compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, confidential information furnished only by a confidential source,

(e) Disclose investigative techniques and procedures

(f) Endanger the life or physical safety of law enforcement personnel.

(8) Contained in or related to examination, operating or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions.

(9) Geological and geophysical information and data, including maps concerning wells.

21-21.3. In addition to the above, the following types of record information are not releasable under the terms of this NCIS policy: reports from other agencies such as the FBI; adverse information from a close relative or associate which, if disclosed, might cause harm to that individual; medical reports concerning subject wherein a mental illness or defect is diagnosed; and medical reports/records concerning individuals other than subject.

21-21.4. The complete investigative report will be provided to the requesting command even though it contains non-releasable record information. The Document Control Sheet (DCS) transmitting the investigative reports denies their use to a subject or his counsel without express authorization from the servicing NCIS Field Office/Resident Agency.

21-21.5. Release of record information pursuant to this policy is not deemed to be "granting or denial" under the provisions of the Privacy Act since this is an initiative action by NCIS. This policy is not applicable in overseas areas in those cases in which the subject of the investigation is a foreign national not subject to the laws of the United States.

21-22. INQUIRES CONCERNING REQUESTERS PROHIBITED

Individuals who make requests under the Privacy Act will not be questioned concerning their motives nor will any file checks, inquiries or investigations of any kind be conducted concerning those requesters or their motives.

21-23 ACCESS TO NAVY RECORDS BY NCIS PERSONNEL

21-23.1. See Navy Privacy Act Office (Website Address: http://privacy.navy.mil/)

21-23.2. Established blanket routine uses are applicable to every record system maintained within the DON unless specifically exempted within a particular system of records. The blanket routine uses provided for all systems of records in the Navy that deal with law enforcement provides that:

"In the event that a system of records maintained by a Navy component to carry out its functions indicates a violation or potential violation of law . . . the relevant records in the system of records may be referred as a routine use to the appropriate agency, whether federal, state, local, or foreign, charged with the responsibility of investigating or prosecuting such violation . . ."

21-23.3. SECNAVINST 5211.5E, Section 13.a. provides that disclosure may be made to personnel of the Department of Defense who have a need for the record in the performance of their duties, based on a need to know concept.

21-23.4. Contact NCIS Code 00L for assistance if access to records must be denied during the course of an investigation and citation of the SECNAVINST fail to produce results.

21-24 NCIS INVESTIGATIVE FILES SYSTEMS NOTICE

21-24.1. SYSTEM NAME. NCIS INVESTIGATIVE FILES SYSTEM (June 30, 1998, 63 FR 35578)

21-24.2. SYSTEM LOCATION

a. Primary System: Director, Naval Criminal Investigative Service, 716 Sicard Street, S.E., Suite 2000, Washington Navy Yard DC, 20388-5380.

b. Decentralized Segments: NCIS field offices retain copies of certain portions of some investigative files and related documentation for up to one year. NCIS Resident Agencies retain copies of investigative reports during pendency and for one year thereafter. They also retain evidence custody cards on person from whom evidence was seized. The number and location of these Resident Agencies are subject to change in order to meet the requirements of DON.

c. Consolidated Evidence Facilities: Consolidated Evidence Facilities maintain evidence inventory records.

d. Current locations of NCIS decentralized segments may be obtained from the Director, Naval Criminal Investigative Service, Washington Navy Yard, 716 Sicard Street, S.E., Suite 2000, Washington Navy Yard, DC 20388-5380.

21-24.3. Categories of Persons Covered by the System. Persons in the following categories who require access to classified defense information prior to August 1972: Active and inactive members of the naval service, civilian personnel employed by the DON, industrial and contractor personnel, civilian personnel being considered for sensitive positions, boards, conferences, etc., civilian personnel, who worked or resided overseas and Red Cross personnel. Civilian and military personnel accused, suspected, or victims of felonious type offenses, or lesser offenses impacting on the good order, discipline, morale or security of the DON; civilian personnel seeking access to or seeking to conduct or operate any business or other function aboard a DON installation, facility or ship; civilian or military personnel who are subjects, co-subjects, and victims in law enforcement and investigative cases in which law enforcement and investigative authorities (Federal, state, and local) have requested laboratory analysis of submitted evidence for

law enforcement purposes; civilian and military personnel upon whom evidence is stored at a Consolidated Evidence Facility; civilian or military personnel involved in the loss, compromise, or unauthorized disclosure of classified material/information; civilian and military personnel who were of counterintelligence interest to DON.

21-24.4. Categories of Records in the System. Official Reports of Investigation (ROI) prepared by NCIS or other federal, state, local or foreign law enforcement or investigative body. Predecessor NCIS operations reports (NORs) and their predecessor NCIS information reports (NIRs). NORs and NIRs document information received by NCIS, which is of interest to the naval services or other law enforcement or investigative bodies. The information may be of criminal, counterintelligence, or general investigative interest. General Reports (GEN), although no longer used as such, the investigative purpose of the GEN was to report the results of pre-employment inquiries on applicants for positions as special agents with NCIS. The official ROI is now used for this purpose. Predecessor Action Lead Sheets (ALS's), investigative summaries, memoranda for the files and correspondence relating to specific cases and contained in the individual dossier. Polygraph Data. A listing of persons who submitted to polygraph examination by NCIS examiners. The data includes the examinee's name, location and results of the examination and the identity of the examiner. Case Control and Management documents that serve as the basis for controlling and guiding the investigative activity. (Records identifying confidential sources and contacts with them. Index to persons reported by 'Name Only'.) Regional Laboratory Report Records. Records reporting and documenting laboratory analysis of submitted evidence. Consolidated Evidence Inventory Records. Reporting and documenting evidence analyzed, stowed, transferred, or destroyed. (Wiretap Data Records. Automated listing of persons who were subjects of wiretapping or eavesdropping operations.) Case Control and Narcotics Data Records. Automated records used only for statistical purposes in accounting for productivity, man-hour expenditures; various statistical data concerning narcotics usage and used solely for statistical purposes. Screening Board Reports. These reports set forth the results of oral examination of applicants for a position as a special agent with NCIS.

21-24.5. Authority for Maintenance of the System. 5 U.S.C. 301 and 10 U.S.C. 5013, Departmental Regulations; 44 U.S.C. 3101; 47 U.S.C. 605; Executive Memorandum of June 26, 1939, Investigations of Espionage, Counterespionage and Sabotage Matters; DoD Directive 5210.8, Policy on Investigation and Clearance of DoD Personnel for Access to Defense Information; DoD Directive 5200.24, Telephone Interception and Eavesdropping; DoD Directive 5200.26, DSS Program; DoD Directive 5200.27, Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense; Secretary of the Navy Instruction 3820.2D, Investigative and Counterintelligence Collection and Retention Guidelines Pertaining to the Department of the Navy; Secretary of the Navy Instruction 5520.3, Criminal and Security Investigations and Related Activities Within the Department of the Navy; E.O. 9397; and E.O. 13292, United States Intelligence Activities.

21-24.6. Purpose(s). The information in this system is (or was) collected to meet the investigative, counterintelligence, and security responsibilities of the DON. This includes personnel security, internal security, criminal, and other law enforcement matters all of which are essential to the effective operation of the Department. The records in this system are used to make determinations of: suitability for access or continued access to classified information; suitability for access to

military installations or industrial firms engaged in government projects/contracts; suitability for awards or similar benefits; use in current law enforcement investigation of any type including applicants; use in judicial or adjudicative proceedings including litigation or in accordance with a court order; insurance claims including workmen's compensation; provide protective services under the DoD Distinguished Visitor Protection Program and to assist the U.S. Secret Service in meeting its responsibilities; used for public affairs or publicity purposes such as wanted persons, etc.; referral of matters under their cognizance to federal, state or local law enforcement authorities including criminal prosecution, civil court action or regulatory order; advising higher authorities and naval commands of the important developments impacting on security, good order or discipline; reporting of statistical data to naval commands and higher authority; input into the DCII. Users of the records in this system include NCIS employees who require access for operational, administrative, or supervisory purposes; DoD criminal investigative and intelligence units; DoD components making suitability determinations.

21-24.7. Routine uses of Records Maintained in the System, Including Categories of users and the Purposes of such uses. In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. a(b)(3) as follows: To law enforcement or investigatory authorities for law enforcement purposes. To federal intelligence/counterintelligence agencies of matters under their purview. To foreign government organizations of criminal and counterintelligence information necessary for the prosecution of justice, or for mutual security and protection. To other investigative units (federal, state, or local) for whom the investigation was conducted, or who are engaged in regulatory, criminal investigative and intelligence activities; to defense counsel in the course of acquiring information. To officials and employees of the National Archives for historical purposes. To commercial insurance companies in those instances in which they have a legitimate interest in the results of the investigation, but only to that extent and provided an unwarranted invasion of privacy is not involved. To victims of crimes to the extent necessary to pursue civil and criminal remedies. The 'Blanket Routine Uses' that appear at the beginning of the Navy's compilation of systems notices also apply to this system.

21-24.8. Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records.

a. Storage. Paper and automated records.

b. Retrievability. NCIS permanent files are filed by terminal digit number. In order to locate the file it is necessary to query the DCII computer using the name of the subject and at least one other personal identifier such as date of birth, place of birth, or Social Security Number. A case control number assigned at the time the investigation is initiated may also retrieve files. Copies of the files in the NCIS field office and Resident Agencies are retrieved by name. Consolidated Evidence Facility and Regional Forensic Lab information is retrieved by name, case control number, submitting agency log number, log numbers, or lab numbers.

c. Safeguards. NCIS investigative files (permanent and temporary) are maintained and stored in open shelves and filing cabinets located in secured areas accessible only to authorized personnel. Controls have been established to restrict computer output to only authorized users at all system

locations. Computer records are kept in secure, continually manned areas and are accessible only to authorized computer operators. Dated files are retired to the Washington National Records Center where retrieval is restricted to NCIS authorized personnel.

d. Retention and Disposal. Retention of completed NCIS investigative files on Personnel Security Investigations (PSI's) is authorized for 15 years unless adverse information is developed, in which case they may be retained for 25 years. PSI files on persons considered for affiliation with DoD will be destroyed within one year if the affiliation is not consummated. Special Agent applicant records are retained for one year if the applicant declines offer of employment and five years if the applicant is rejected for employment. Criminal files are retained for 25 years. Major investigations of a counter-intelligence/security nature, of espionage or sabotage, may be retained permanently. Investigations to have possible historical value may be offered to the National Archives for continued retention. Counterintelligence records on persons not affiliated with DoD must be destroyed within 90 days or one year under criteria set forth in DoD Directive 5200.27, unless retention is required by law or specifically approved by SECNAV. Decentralized consolidated evidence files and decentralized laboratory report files are destroyed after 5 years unless circumstances require longer retention. Files retained in the NCIS field offices and Resident Agencies are temporary and are destroyed after 90 days or one year, as appropriate.

21-24.9. System Manager(s) and Address. Director, Naval Criminal Investigative Service, 716 Sicard Street, S.E., Suite 2000, Washington Navy Yard DC, 20388-5380 has ultimate responsibility for all NCIS file holdings. Management of NCIS permanent files is the direct responsibility of the Head, Administration Department Code 11C. Regional directors are responsible for files retained in their NCIS field office subordinate Resident Agencies.

21-24.10. Notification Procedure. Individuals seeking to determine whether this system of records contains information about themselves should address written inquiries to the Director, Naval Criminal Investigative Service, 716 Sicard Street, S.E., Suite 2000, Washington Navy Yard, DC 20388-5380. Requests must contain the full name of the individual and at least one additional, personal identifier such as date and/or place or birth, or Social Security Number. Persons submitting written requests must properly establish their identity to the satisfaction of the NCIS. Either submitting a notarized signature or providing an unsworn declaration that states ‘I declare under perjury or penalty under the laws of the United States of America that the foregoing is true and correct’ can accomplish this. Attorneys or other persons acting on behalf of a subject of a record must provide a notarized authorization from the subject of the record.

21-24.11. Procedures. Individuals seeking access to records about themselves contained in this system of records should address written inquiries to the Director, Naval Criminal Investigative Service, 716 Sicard Street, S.E., Suite 2000, Washington Navy Yard DC, 20388-5380. Requests must contain the full name of the individual and at least one additional personal identifier such as date and place of birth and Social Security Number. Persons submitting written requests must properly establish their identity to the satisfaction of the NCIS. Either submitting a notarized signature or providing an unsworn declaration that states “I declare under perjury or penalty under the laws of the United States of America that the foregoing is true and correct” can accomplish this. Attorneys or other persons acting on behalf of a subject of a record must provide a notarized authorization from the subject of the record.

21-24.12. Contesting Record Procedures. DON rules for accessing records, and for contesting contents and appealing initial agency determinations are published in Secretary of the Navy Instruction 5211.5.32 CFR part 701; or may be obtained from the system manager.

21-24.13. Record Source Categories. Individuals concerned, other records of the activity, investigators and witnesses.

21-24.14. Exemptions Claimed for the System. Parts of this system may be exempt pursuant to 5 U.S.C. 552a(j)(2) and (k)(1), (k)(3), (k)(4), (k)(5), and (k)(6), as applicable. An exemption rule for this system has been promulgated in accordance with requirements of 5 U.S.C. 553(b)(1), (2), and (3), (c) and (e) and published in 32 CFR part 701, subpart G. For additional information, contact the system manager.

21-25 NCIS ADMINISTRATIVE FILES SYSTEM

21-25.1. System Name. NCIS ADMINISTRATIVE FILES SYSTEM (February 22, 1993, 58 FR 10702)

21-25.2. System Location.

a. Primary: Director, Naval Criminal Investigative Service, 716 Sicard Street, S.E., Suite 2000, Washington Navy Yard DC, 20388-5380.

b. Decentralized Segments: NCIS field offices retain duplicate copies of certain segments of the administrative files. Official mailing addresses are published as an appendix to the Navy's compilation of system of records notices.

21-25.3. Categories of Individuals Covered by the Systems. Past and present civilian, military, and foreign national personnel assigned worldwide to the NCIS.

21-25.4. Categories of Records in the System.

a. Personnel and Resource Information System - contains personnel management information/statistical information on NCIS personnel.

b. Special Agent Career Development Files - contains correspondence unique to the NCIS Special Agent, including annual physical examinations, assignment preferences, and special qualifications, which has a bearing on world-wide assign ability, promotion, and general career assessment.

c. Weapons and Equipment Files - identifies credential numbers, badges, PSP pins, and weapons assigned to authorized NCIS personnel.

d. Personnel Security Clearance File - identifies the classified material access level and date of last security clearance for assigned civilian and military personnel of NCIS.

e. Personnel Utilization Data File - provides statistical information regarding the manner by which available NCIS man-hours are expended in the execution of its assigned investigative and counterintelligence mission. The file is formed by the submission (monthly) of individual man-hour diaries. All assigned personnel input to this system; their man-hours are categorized by function.

f. Freedom of Information Act and Privacy Act Requests File -contains correspondence and responses made to requests for information pursuant to the Freedom of Information Act and the Privacy Act of 1974.

21-25.5. Authority for Maintenance of the System. 5 U.S.C. 301, Departmental Regulations and E.O. 9397.

21-25.6. Purpose. The Personnel and Resource Information System is used to prepare all personnel documents and personnel statistical studies. It provides such information as the average grade, the total number and composition of personnel at each NCIS component, and the past assignments of personnel. Personnel in the formation and execution of staffing actions for the various NCIS components, information verification of employee's tenure, and the compilation of necessary statistical studies use it on a daily basis. Special Agent Career Development Files are used for in-house agency decisions regarding reassignment, promotion, career training, and long-range development. They form in-house agency repository for both adverse and favorable documents regarding Special Agents. The files have a long-range function that of forming the basis for law enforcement retirement service certification. Though part of the file is duplicated in the official file maintained by the Civilian Personnel Office, the Special Agent Career Development File is considered privileged information and its contents are not released outside NCIS. Within NCIS, the files are maintained and controlled exclusively within the Career Services Division, NCIS, and by assigned personnel of that Division. The files are released for review only to senior management personnel of NCIS. Weapons and Equipment Files are used to identify and inventory credentials, weapons, badges, and handcuffs issued to authorized NCIS personnel. Personnel Security Clearance Files are used to informally verify and authenticate security clearances issued to NCIS personnel. The file has a daily working purpose of acting as a check sheet for the updating of security clearances. The Director, NCIS uses it, to certify the access level of certain assigned NCIS personnel to other Navy commands as well as civilian contractors. Personnel Utilization Data File is used to make analyses, which modify the staffing levels at various NCIS components based on the actual work level. It further provides a tool to NCIS management to gauge the efficiency of all components by comparing their workload with the amount of man-hours available. The records in this system may be used by other DoD components requiring confirmation of security clearance levels and for statistical purposes. Freedom of Information Act and Privacy Act Request Files are used to record actions taken on requests/appeals/amendments.

21-25.7. Routine uses of Records Maintained in the System, Including Categories of users and the Purposes of Such Uses.

a. In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the DOD as a routine use pursuant to 5 U.S.C.552a (b)(3) as follows:

(1) To law enforcement activities conducting criminal or suitability investigations.

(2) To the Office of Personnel Management when making personnel determinations; e.g., awards or disciplinary actions.

(3) To credit companies in response to credit queries.

(4) To personal physicians regarding medical records.

b. The ”Blanket Routine Uses” that appear at the beginning of the Navy's compilation of systems notices also apply to this system.

21-25.8. Policies and Practices for Storing, Retrieving, Accessing, Retaining, and Disposing of Records in the System.

a. Storage. Automated and paper records.

b. Retrievability

(1) For the Special Agent Career Development File - name only.

(2) For the Weapons and Equipment File - by name or by item number (i.e., badge, credential, weapon, handcuff serial number).

(3) For the Personnel and Resource Information System - by name and Social Security Number or by individual data characteristic, such as GS-grade level, duty-station, special qualifications, or language qualifications.

(4) For the Personnel Utilization Data File - normally accessed and retrieved by location and functional category of employment (i.e., Special Agent, clerical, etc.). The capability exists, however, to retrieve by Social Security Number. Name and Social Security Number access the Personnel Security Classification File, which is a subordinate file to the Personnel and Resource Information System.

(5) For the Freedom of Information Act and Privacy Act Requests File - by name and year request was made.

c. Safeguards. Files are protected by limited controlled access, safes, locked cabinets, and locked doors. Visitor control and security computer software measures (where applicable) are utilized.

d. Retention and Disposal.

(1) Personnel indexed in the Personnel and Resource Information System and the Personnel Security Clearance Files are deleted from the magnetic tape data storage upon termination of employment. Residual paper records are retained from two to five years and then destroyed.

(2) Personnel indexed in the Weapons and Equipment Files are deleted as assigned equipment is accounted for or returned. Residual paper printouts are destroyed at least semi-annually.

(3) The Special Agent Career Development Files are semi-permanent and area retained, at least in essential skeletal format, indefinitely.

(4) Personnel indexed in the Freedom of Information Act and Privacy Act Requests File are deleted after two years if their request was granted or no record found and six years if the request was denied in whole or in part.

21-25.9. System Managers and Address. Director, Naval Criminal Investigative Service, 716 Sicard Street, S.E., Suite 2000, Washington Navy Yard DC, 20388-5380.

21-25.10. Notification Procedures. Individuals seeking to determine whether this system of records contains information about themselves should address written inquiries to the Director, Naval Criminal Investigative Service, 716 Sicard Street, S.E., Suite 2000, Washington Navy Yard, DC, 20388-5380. Individuals submitting requests should provide their full name, date of birth, Social Security Number, and dates of employment or assignment with NCIS. In the case of personal visits, individuals requesting access to files in this system will be required to present reasonable proof of identity to minimally include a driver's license or similar document at least one of which must bear a current photograph and be able to provide (orally) some element of unique identifying data such as name of spouse or a past duty-station with NCIS.

21-25.11. Record Access Procedures. Individuals seeking access to records about themselves contained in this system of records should address written inquiries to the Director, Naval Criminal Investigative Service, 716 Sicard Street, S.E., Suite 2000, Washington Navy Yard DC, 20388-5380. Individuals submitting requests should provide their full name, date of birth, Social Security Number, and dates of employment or assignment with NCIS. In the case of personal visits, individuals requesting access to files in this system will be required to present reasonable proof of identity to minimally include a driver's license or similar document at least one on which must bear a current photograph and be able to provide (orally) some element of unique identifying data such as name of spouse or past duty-station with NCIS.

21-25.12. Contesting Record Procedures. The Navy's rules for accessing records and for contesting contents and appealing initial agency determinations are published in Secretary of the Navy Instruction 5211.5; 32 CFR Part 701; or may be obtained from the system manager.

21-25.13. Record Source Categories.

a. Information for the Personnel and Resource Information System and the Personnel Utilization Data System is obtained from the individual employee, who is the prime source of information both for initial access to the files as well as for the periodic update.

b. Information for the Personnel Security Clearance File information is obtained from the Personnel and Resource Information System.

c. The information for the Weapons and Equipment Files is obtained from personnel charged with the issuance of various items inventoried therein (with verification by the personnel to whom the items are issued.)

d. Information for the Special Agent Career Development File is obtained from the individuals' supervisors, from various naval commands, and other federal and state agencies with whom the special agent has had professional contact and from the individual. Also, this file contains copies of each physical examination required annually of assigned civilian special agents.

e. Information for the Freedom of Information Act and Privacy Act Requests file is obtained from the individual requesting the information.

21-25.14. Exemptions Claimed for the System. None

CHAPTER 22
TITLE: NAVAL CRIMINAL INVESTIGATIVE SERVICE CLOSED CASE FILES
POC: Code 11C1
DATE: JULY 07

22-1. GENERAL

22-1.1. The Records Management Branch (RMB) Code 11C1 of the Naval Criminal Investigative Service Headquarters (NCISHQ), has the responsibility to ensure proper maintenance and availability of closed NCIS criminal, counterintelligence (CI) and counterterrorism (CT) investigations and operations, USMC and Navy Criminal Investigation Division (CID) criminal investigations, and the Department of the Navy Central Clearance Facility (DON CAF) case files. Additionally, RMB stores Navy and Marine Corps information reports (IR) from 1 January 1996 forward.

a. Closed case files will be sent to NCIS Headquarters, except as specified below. Files will be sent by the most practical means consistent with security guidance and the safety of the package. In cases where the case or portions thereof are damaged, the submitting Field Office will be notified to resubmit a replacement. When submitting closed cases to RMB, NCIS offices and codes must follow the guidance contained in Case Management Guidance for Sending Routine Closed Cases Files to RMB, located on the NCIS Info-Web under Case Management Guidance. The following specific guidance applies:

(1) Routine closed case files, to include investigations completed by Code 10, will be sent directly to NCIS Headquarters, RMB Files Section, NCIS Code 11C12. When cases to be mailed are classified, the submitting Field Office will send an e-mail via NIPRNet to "11C12 Files Section" identifying by case number the files contained in the package. A copy of that e-mail will be included in the package. Upon receipt, Files Section will respond acknowledging receipt. The receipt e-mail will cc the appropriate operational Codes; 21C, 22, 24D as necessary.

(2) Certain categories of closed cases will not be forwarded directly to RMB. Field Offices will continue to submit these cases to the cognizant NCISHQ code. Submission of these cases by NCISHQ codes to RMB must also follow the Case Management Guidance contained in the NCIS Info-Web, cited above. These categories are:

(a) Director Special Interest (DSI) and Special Interest (SI) cases.

(b) Tiger Collar cases, which are sent to Code 22. (These cases are not currently submitted to RMB.)

(c) Death investigations (7H), which are sent to Code 23.

(d) Terrorism investigations (5T) and Counterterrorism Collection operations (XXCT), are sent directly to Code 21B.

(3) Incident Reports received from Navy Law Enforcement, USMC Provost Office and Navy and USMC CID offices are mailed to "IR Project" and are passed to Imaging Branch, Code 11C13, for incorporation into the NCIS electronic closed case management system.

b. Once files are integrated into RMB, they are maintained in dossiers on open shelving, on microfilm or as images on optical disk located at NCISHQ RMB, Records Center (RC). Files for which there is insufficient space to store at the RMB, RC are stored at the Washington National Records Center WNRC located in Suitland, MD.

c. The optical disk system, known as the Records and Information Management System (RIMS) is operational and access is limited to NCISHQ and other selected sites. Access to RIMS is available to NCIS Field Offices (FOs) upon request. The RIMS system is being populated with cases. While most of the cases are those created from 1999 to date, there are numerous older cases dating to the 1960s in the system. Eventually all hardcopy and microfilm holdings will be converted to optical images in RIMS.

d. Plans have been developed for a classified version of RIMS, called the Classified Records and Information Management System (CRIMS). When CRIMS is fielded, it will contain all case files, classified (up to SECRET) and unclassified. CRIMS will be available in those locations that can provide the necessary security. In the meantime, access to classified records must be requested using procedures established in NCIS-1, Chapter 23.

22-1.2. RETENTION STANDARDS. Retention standards are assigned to the various records series in accordance with retention and disposition guidance published in SECNAV Manual 5210.1, Records Management Manual, Part III. Some changes to NCIS records series and retention periods have been approved by the Archivist of the United States, National Archives and Records Administration (NARA) and will be included in the next revision to the SECNAV Manual. Using the retention guidelines contained in SECNAV M-5210.1, RMB personnel accomplish an annual review of files that have reached their retention limit. Files that have aged-out are destroyed/deleted, or if determined to hold historical value, permanently transferred to the NARA.

22-1.3. DISSEMINATION. Original files are not disseminated outside NCISHQ, Building 111 unless specifically authorized by the Deputy Director, Management & Administration (01) or higher authority. Only reproduced copies of the files are distributed to authorized requesters.

NCISHQ activities located outside Building 111 authorized to receive original files are Codes 10B and 23B, Cold Case and Polygraph offices and the Office of Special Projects (Code 22O).

22-2. NAME FILES

Name files are files that contain investigative, counterintelligence, counterterrorism, and or other security related information concerning an individual, either a U.S. citizen or foreign national. Name files are assembled into dossiers, which are filed by assigned numbers with files physically located on open shelves. These cases also exist on microfilm or on optical disk within the RMB, and at the WNRC. Original material committed to imaging is destroyed, with certain exceptions such as crime scene color photographs, after it has been committed to optical disk and quality checked.

22-3. IMPERSONAL TITLE FILES

Impersonal title files (also know as I-Titles) concern U.S. and foreign organizations and companies that are affiliated or nonaffiliated with the DOD. These files are filed in alphabetical sequence in the RMB,. Impersonal title files are physically located on open shelves. These cases also exist on microfilm or on optical disk within the RMB, or at the WNRC. Original material committed to imaging is destroyed, with certain exceptions such as crime scene color photographs, after it has been committed to optical disk and quality checked.

22-4. TOPICAL FILES

22-4.1. Topical files pertain to investigative and counterintelligence information regarding certain incidents or crimes occurring at, or aboard, particular commands or activities.

a. Topical files are filed by case control number.

b. Topical files are physically located in Lektrievers or on open shelves. These cases also exist on optical disks located within RMB. Original material committed to imaging is destroyed, with certain exceptions such as crime scene color photographs, after it has been committed to optical disk and quality checked.

22-5. SPECIAL CONTROL FILES

Dossiers placed under special control are files determined to require restricted access. Commonly called Controlled Files, these include files on high ranking government officials such as Navy Statutory appointees, elected officials and DON employees holding excepted positions; incumbent NCIS employees; specifically designated impersonal title files concerning certain counterintelligence/counterespionage/counterterrorism (CI/CE/CT) operations; specifically designated sensitive topical files and files designated by NICSHQ Deputy Assistant Directors or higher officials. These dossiers are filed in alphabetic sequence within the RMB, in security containers approved for the storage of classified material and physically separate from the other master name, impersonal and topical files. At a future date control files will be imaged and stored on optical disk. Access will be password protected and limited to persons specifically

authorized access in writing. Refer to NAVCRIMINVSERINST 5211.4G, November 2005, Procedures for Special Control Files, for details. The Head of the RMB is the custodian of Special Control Files.

22-6. ACCESS AUTHORIZATION

22-6.1. Recognized access authorization includes persons having access to NCISHQ files. "Access" is defined as authority to withdraw and review contents of NCISHQ files, as well as to request or conduct DCII searches**.** For persons authorized to carry NCISHQ files, "Carry" is defined as authority to pick up NCISHQ files from the RMB, and deliver to those authorized to review. .

a. Access to RIMS requires a two-step approval process:

(1) The individual must have written approval for access to closed case files and

(2) The individual must be approved in writing to be given RIMS access using a government computer, and Code 15, or the RMB system administrator, must enter the person into the appropriate RIMS GROUP.

b**.** The form necessary to obtain approval for access and carry of dossiers and access to RIMS are contained on the NCISnet under the “Administrative Forms” button.

(1) Access/Carry: This form is labeled “Access/Carry Authorization to Naval Criminal Investigative Service Files” (NCIS Form 5211.104). Refer to paragraph 22-6.1, above, and NAVCRIMINVSERVINST 5211.1F for guidance for completing this form.

(2) RIMS: This form is labeled “Application Access Form” (CIS, FMS, PARIS, RIMS). Both the “Access/Carry” and “System Access Form” are necessary for electronic access to NCIS files. The completed form must be submitted to the Head or Assistant Head RMB for approval. RMB will notify Code 15 for completion of the installation/access process for approved access requests. Approved RIMS users may request training from the Head RMB.

22-6.2. RESPONSIBILITIES

a. Access/Carry Designation. Deputy Assistant Directors are responsible for designating personnel in their departments for access/carry authorization in the performance of their duties, and for providing controls within their department to ensure that NCISHQ files are reviewed only on an official need-to-know basis. NCISHQ DADs must ensure that only a limited number of personnel are designated for access and/or carry authorization to Control Files. Supervisors are responsible for designating personnel for access to files via RIMS RIMS access will only be granted for persons who have been approved for access/carry.

b. Safeguarding. All NCISHQ files must be carefully safeguarded during loan periods. NCISHQ DADs must ensure that only a limited number of personnel are designated for access and/or carry authorization to Control Files. Control Files, in sealed envelopes, will be hand

carried to and from the RMB custodian as prescribed in NCISHQINST 5211.4G. Failure to properly safeguard files, from those not authorized to see or access controlled case files, can result in the loss of access/carry privileges.

c. Personal Responsibility for Loaned Files. Individuals charged for a file are personally responsible for the file until it is returned to RMB, or when custody is transferred to someone else. RMB must be notified of file transfer via NCIS Form 5210-20 (Rev 03/00) (Charge Card) when a file is transferred within a department or to another NCISHQ department. Form 5210-20 will be filled out with all pertinent information regarding the file and marked "RECHARGE" in the upper right-hand corner of the form. Change of custody is not complete until the Files Section of RMB, has received Form 5210-20. It is the responsibility of the person transferring custody to ensure that the Form 5210-20 is delivered to Files Section.

d. Electronic Access. Persons approved for access to NCIS closed case files and RIMS may access files using RIMS.

e. Restrictions.

(1) Individuals cannot access their own file, or those of immediate family members or other relatives. Requests for access to an individual personal files may be requested in writing to NCISHQ FOIA Code 00LJF, located at 716 Sicard Street SE Suite 2000, Washington DC 20388-5380.

(2) Restrictions on the dissemination of electronic case file information are the same as for hardcopy dossiers.

22-7. ASSISTANCE

22-7.1. General assistance may be requested by contacting the Head RMB (11C1) at (202) 433-9505, DSN 288-9505 or to the Assistant Head (11C1X) at (202) 433-9520, DSN 288-9520.

Appendix 1

DATE: _____

To: Head, Records Management Branch (Code 11C1)

Subj: ACCESS/CARRY AUTHORIZATION TO NAVAL CRIMINAL INVESTIGATIVE SERVICE (NCIS) FILES

1. The following named personnel are authorized to handle NCIS files in the manner indicated. If access to Control Files (2B) is needed, this document must also be approved and signed by the Inspector General (00I). Refer to NCISHQINST 5211.1E, Paragraph 5, for details.

NAME (TYPED & SIGNATURE) (Last, First, MI)	OFFICE CODE	NAME/ TOPICAL FILES	CONTROL FILES	CONTROL FILES (2B)
1._____ TYPED NAME OF INDIVIDUAL _____ SIGNATURE		☐ Access ☐ Carry	☐ Access ☐ Carry	☐ Access ☐ Carry
2._____ TYPED NAME OF INDIVIDUAL _____ SIGNATURE		☐ Access ☐ Carry	☐ Access ☐ Carry	☐ Access ☐ Carry
3. _____ TYPED NAME OF INDIVIDUAL _____ SIGNATURE		☐ Access ☐ Carry	☐ Access ☐ Carry	☐ Access ☐ Carry
4. _____ TYPED NAME OF INDIVIDUAL _____ SIGNATURE		☐ Access ☐ Carry	☐ Access ☐ Carry	☐ Access ☐ Carry

2. POC for the above is _____ at

telephone number _____.

APPROVED: _____
Director, Deputy Director, Assistant Director, or Deputy Assistant Director
(Typed Name)

SIGNATURE:_____

For Access to control Files (2B).

APPROVED/DISAPPROVED: _____
Inspector General
(Typed Name)

SIGNATURE:_____

Appendix 2

Naval Criminal Investigative Service
Application Access Form

USER INFORMATION

Last Name _____ **First Name** _____ **MI** __

Office Code _____ **Telephone (Comm/DSN)** _____

APPLICATION ACCESS
(USE A SEPARATE FORM FOR EACH APPLICATION REQUESTED)

CIS : ☐ Add* ☐ Remove **PARIS:** ☐ Add* ☐ Remove
FMS : ☐ Add* ☐ Remove **RIMS :** ☐ Add* ☐ Remove

* I certify that this individual has a valid need to access the above application in order to meet job requirements.

_____ _____
Supervisor Signature **Date Signed**

PROGRAM SPONSOR
(APPLICATION ACCESS REQUESTS MUST BE SUBMITTED TO THE IT DEPARTMENT BY PROGRAM SPONSOR ONLY)

PARIS [Dan D'Ambrosio] FMS [Ken Burns] CIS [Harlan Rossman]
RIMS [Henry Persons]

_____ _____
Sponsor Signature **Date Signed**

ACCESS LEVEL

CIS (Criminal Investigations Directorate Use Only)
☐ **View** ☐ **Modify**

FMS (Comptroller Use Only)
☐ **ACCTING**
☐ **ADMIN**
☐ **BUDGET**
☐ **PROCUREMENT**
☐ **DEPARTMENT**
☐ **FIELD OFFICE**

PARIS (Personnel Operations & Services Department (POSD) Use Only)

☐	**PARIS**	Full unlimited access (POSD only)
☐	**FIELD OFFICE**	Allows field office managers limited access to update information for employees in their area
☐	**BENEFITS**	Allows modification access to Benefits & Equipment Screens (POSD only)
☐	**TRAINING**	Full access to the Training screen
☐	**SECURITY**	Full access to the Security screen
☐	**AGENT25**	Access to items unique to agents (POSD only)
☐	**MANAGER**	View only access to all NCIS employee information
☐	**EEO**	Full access to EEO screen
☐	**TECH**	Tech Services Field Office level and Weapons screen (Tech Services Division only)
☐	**MILITARY**	Full access (Code 41 only)

RIMS (Records Management Use Only)

☐ **CASE INFO** ☐ **View** ☐ **Modify**

IT DEPARTMENT INSTALLATION INFORMATION

_____ _____ _____

IT Department Signature

NCIS 1, CHAPTER 23
DEFENSE CENTRAL INDEX OF INVESTIGATIONS (DCII)
EFFECTIVE DATE: JUNE 2014

TABLE OF CONTENTS **PAGE**

References:

(a) DoDI 5505.7, Titling and Indexing of Subjects of Criminal Investigations in the DoD, January 27, 2012
(b) DoDI 5200.2-R, Personnel Security Program, January 1987
(c) DoDI 8500.2, Information Assurance (IA) Implementation, February 6,2008
(d) SECNAV M-5210.1, DON Records Management Program, Records Management Manual January 2012

23-1. Purpose. This chapter provides policy and procedural guidance for obtaining access to the Defense Central Index of Investigations (DCII) and for indexing NCIS and Department of Navy (DON) investigative counterintelligence, counterterrorism, and criminal law enforcement reports and security clearance adjudicative case information in the DCII. This chapter describes procedures used to conduct a file search and retrieve closed case files maintained by the NCIS Headquarters (NCISHQ) Records Management Branch (RMB), Code 11C1. The provisions of this chapter apply to civilian employees, active duty and reserve military personnel and contractors.

23-2. Policy. NCIS HQ Records Management Branch (RMB) is responsible to maintain, control, and manage NCIS closed case files and accomplish the disposal of these records in accordance with guidance for each specific record series. Reference (a) establishes mandatory policy guidance for indexing in the DCII the subjects of criminal investigations when a determination that credible information exists that a person or entity may have committed a criminal offense or is otherwise made the subject of a criminal investigation (See definition for credible information in paragraph 23-6a below). It is also DoD policy that Defense Criminal

Investigative Organizations (DCIOs) and other DoD law enforcement organizations that conduct criminal investigations shall place the names and identifying information of people under criminal investigation in the title blocks of investigative reports.

a. All names of individual subjects of criminal investigations by DoD organizations shall be listed in the DCII. Titling and indexing in the DCII shall be done as soon as the investigation determines that credible information exists that the subject committed a criminal offense. This policy does not preclude the titling and indexing of victims or incidentals associated with criminal investigations.

b. The acts of titling and indexing are administrative procedures and shall not connote any degree of guilt or innocence. Judicial or adverse administrative actions shall not be taken against individuals or entities based solely on the fact that they have been titled or indexed due to a criminal investigation.

23-3. Cancellation. NCIS 1, Chapter 23, August 2007.

23-4. Chapter Sponsor. The Administrative Services Department, Code 11C, sponsors this chapter.

23-5. General Information

a. The DoD established the DCII at the direction of the Secretary of Defense to act as a computerized central index of investigations for all DoD investigations and is under the operational control of the Defense Manpower Data Center (DMDC). Reference (b) established the DCII as the single, automated central repository that identifies investigations conducted by DoD investigative agencies and personnel security clearance determination actions. Security clearance adjudication actions, until February 2006 in the DCII, have been removed from the DCII. They are contained in the DoD system known as the Joint Personnel Adjudicative System (JPAS). Individuals desiring security clearance adjudication information will have to obtain a JPAS account. Contact the NCIS Security Office (Code 11A) to obtain a JPAS account. Although the security clearance adjudication actions have been removed from DCII, the files associated with making those determinations by the DON Central Adjudication Facility (DONCAF) were entered into DCII until January 27, 2013, when the DONCAF was incorporated into the DoDCAF.

b. This chapter revision cancels the requirement to enter internal NCIS personnel inquiries and employment investigations (2A, 2B, 2S, & 2M) into DCII.

c. The primary purpose for indexing an individual or entity as the subject of a criminal investigation in the DCII is to ensure that information in a report of investigation can be retrieved at some future time for law enforcement, counterintelligence (CI), counterterrorism (CT) and security purposes. The DCII serves as the index for locating DON CI/CT/CIO, and DON law enforcement investigation case files that are managed by the NCIS RMB.

d. DCII Contributors. Besides NCIS, there are numerous contributors to the DCII. Among these are the Air Force Office of Special Investigations, the U.S. Army Investigative

Records Repository, the U.S. Army Crimes Records Center, the National Security Agency, the DoD Inspector General (DoDIG), the Directorate for Industrial Security Clearance Review, the Defense Logistics Agency, Washington Headquarters Services, the U.S. Coast Guard, the Defense Intelligence Agency, the Defense Office of Hearings and Appeals, the Washington Headquarters Services, the National Reconnaissance Office, and DSS.

e. Agency Responsibility. While Defense Manpower Data Center (DMDC) manages the DCII database, the criminal, CI, counter espionage (CE), CT and other investigative and security clearance adjudication information stored therein remains the record and the responsibility of the contributing agency. Head, Records Management Branch is responsible for DCII policy issues and ultimately for the accuracy of NCIS closed case entries in the DCII.

23-6. Definitions

a. CI Investigations. Includes inquiries and other activities undertaken to determine whether a particular person is acting for, or on behalf of, a foreign power for espionage, treason, spying, sedition, subversion, sabotage, assassinations, international terrorist activities, and actions to neutralize such acts.

b. Credible Information. Information disclosed or obtained by a criminal investigator that, considering the source and nature of the information and the totality of the circumstances, is sufficiently believable to lead a trained criminal investigator to presume that the fact or facts in question are true.

c. Criminal Investigations. Refers to investigations of possible criminal violations of the United States Code, the Uniform Code of Military Justice, or when appropriate, state or local statutes or ordinances or foreign law.

d. Cross Reference. Any person, corporation, organization or entity associated with a matter under investigation other than the "master titled" subject of the investigation or a victim. This term is normally used to identify additional subjects (i.e., co-subjects) of the investigation other than the "master titled" subject.

e. Incidentals. Any person or entity associated with a matter under investigation and whose identity may be of subsequent value for law enforcement or security purposes.

f. Indexing. The procedure whereby an organization responsible for conducting criminal investigations submits identifying information concerning subjects, victims, or incidentals of investigations for addition to the DCII.

g. Subject. A person, corporation, or other legal entity about which credible information exists that would cause a trained criminal investigator to presume that the person, corporation, or other legal entity committed a criminal offense.

h. Tracing. An entry or piece of information in the DCII; includes a case control number, clearance, alias, or a national agency check (NAC).

23-7. DCII Access**.** Access to the DCII is limited to authorized DoD activities and certain non-DoD Federal agencies.

a. Request for DCII Access. To obtain access to DCII, users need to complete and submit a Defense Security Service (DSS) System Access Request Form (DSS 273, June 2011). Forms can be obtained from the DMDC web page: www.dmdc.osd.mil/ psawebdocs/ docPage. jsp?p=DCII. Completed forms should be forwarded to the Security Officer for inclusion of security clearance information and ultimately submitted to the DCII Administrator within NCIS RMB.

b. Security Requirements for the DCII. The DCII is an unclassified system that, under reference (c), is equivalent to Mission Assurance Category II (MAC II). Contributors may only enter unclassified information. Information contained in the DCII shall be protected as required by the Privacy Act.

(1) Due to the sensitive nature of the information, personnel whose primary duties are to input, modify, or delete data shall have a favorably completed SSBI or SSBI-PR. Interim authorization to input, modify, or delete data in the DCII may be granted when the NAC portion of the pending SSBI is favorably completed, the information on the SF-86 is favorable, and no unfavorable information is known. Interim authorization may also be granted if a previous NACI, NAC, NACLC, or ENTNAC has been completed and favorably adjudicated, there is no unfavorable information listed on the SF-86 or otherwise known, and there is no more than 24 months break in service.

(2) Each contributor is responsible for the accuracy of the data he or she enters. Contributors may input, modify, or delete only data originated by them. A contributor may not alter or delete another contributor's information. Each organization is responsible for the accuracy of the data entered by contributors from their respective organization.

(3) Personnel from DoD activities and other Federal agencies authorized "Read Only" access to the DCII shall have, at a minimum, a favorably adjudicated Secret security clearance investigation within the immediately preceding ten years.

(4) Access to DCII shall require the use of a user ID and password. Access to DCII information shall be controlled and limited to those persons authorized access to that information. Access to DCII via assigned user ID and password are for the user’s exclusive use only. By signing the DCII SAR form, the user agrees to protect his or her password from disclosure by all reasonable means, and not to divulge it willingly or permit its use knowingly by another person. If the user believes his or her password has been compromised or used by another person, he or she shall immediately notify his or her supervisor and the NCISHQ RMB DCII Administrator.

(5) Review of information in DCII is for official use only. Users shall not attempt to access their own record in DCII for any purpose, including testing/training situations. Users will not access the record of a coworker, associate or relative without the express approval of their supervisor. Unauthorized access of investigative files or information is prohibited by law, and punishable by a fine of not more than $5,000 (5 U.S.C. 552a). Use of government computers for private or personal use is

prohibited by law and may result in administrative action or criminal prosecution (18 U.S.C. 641; Executive Order 11222).

23-8. Procedures

a. Once an investigation is initiated, the identity of the subject, when known, shall be indexed in the DCII by the controlling NCISHQ code (Code 22 or Code 23) or specifically designated persons. "Open" will be entered in the retention code block.

b. The indexing of "incidentals" in the DCII is not prohibited when there is valid reason. While not normally indexed in the DCII, these records are stored by the NCISHQ RMB and can be retrieved as required. Examples of such indexing are:

(1) Using the name of the person, military installation, command or activity against whom a crime has been committed (i.e., victim) where no suspects have been identified.

(2) Using the name of a project or description of an incident where the focus of an investigation is not a person, corporation or other legal entity or organization.

c. Exceptions to Indexing. Counterintelligence investigations are conducted to protect the national security and by their very nature are extremely sensitive. Law enforcement cases, while rarely rising to this level, nevertheless are occasionally sensitive enough to warrant special precautions so as not to compromise the investigation. Operational security dictates that the knowledge that there is an investigation must be limited to those with a specific need-to-know. Indexing in the DCII would expose the existence of the investigation to individuals who are DCII password holders or to their friends and co-workers. Sensitive CI and law enforcement investigations will not be indexed until such time as the case agent, in coordination with his or her SSA and the applicable HQ directorate, determines that indexing the investigation in the DCII will not compromise the investigation. This is a judgment call and is not to be used to avoid DCII indexing responsibility. Once circumstances warranting the delay no longer exist, indexing will be accomplished within 30 days. The following provides general guidance for, and is not an exhaustive list of, exceptions to indexing cases in the DCII:

(1) When it is believed that the investigation would be compromised during its pendency. This would include internal NCIS personnel inquiry investigations.

(2) Cases involving undercover operations where premature disclosure might place the lives of NCIS or other counterintelligence and law enforcement operatives or family members in danger.

d. Changes and Deletions to DCII

(1) Once the subject of a criminal investigation is indexed, the name shall remain in the DCII, even if a later finding is made that the subject did not commit the offense under investigation, subject to the following exceptions:

(a) Identifying information about the subject of a criminal investigation shall be removed from the title block of a report of investigation and the DCII in the case of mistaken identity; i.e., the wrong person's name was placed in the report of investigation as a subject or entered into the DCII.

(b) Identifying information about the subject of a criminal investigation shall be removed from the title block of a report of investigation and the DCII if it is later determined a mistake was made at the time of the titling and/or indexing occurred, and no credible information indicating that the subject committed a crime existed.

(c) Successful appeals made under paragraph 23-11, below.

(2) Changes. During case pendency, the controlling NCISHQ department will make changes to DCII entries when updating indexed information or correcting an error (e.g., misspelled or incorrect name; incorrect personal identifying data, investigation number, incident report number, Social Security number(s), case status, retention code). Once the case is closed and sent to RMB, only specifically designated RMB individuals are authorized to make changes to DCII entries. The controlling NCSHQ department is authorized to change the status of a closed case when a decision has been made to reopen it. In cases where a user identifies an alleged error, he/she must notify RMB in writing (e-mail is acceptable) identifying the perceived error and citing the reason why the change is believed necessary. Submissions must be made to the Head or Assistant Head of RMB.

(3) Deletions. Normally, deletions of DCII tracings are exclusively the responsibility of the NCIS RMB and are undertaken in conformance with guidance from the Head or Assistant Head of RMB. Other offices authorized DCII access with add, change, and delete authorization, may delete an entry only in cases of an erroneous entry, but only during the pendency of the investigation to update or correct erroneous entries. Within RMB, only specifically authorized persons will undertake deletion actions. Authorized RMB personnel may delete DCII entries:

(a) When a record exceeds it retention period as specified in reference (d) or upon the receipt of an SF 115, Request for Records Disposition Authority, approved by the Archivist of the United States.

(b) In response to a Federal Court Order or other valid legal document ordering the expungement or alteration of the DCII entry. Such documents will be referred to the NCIS legal office for their review and advice before undertaking any change to or deletion of a DCII entry.

(c) When directed by the NCIS Freedom of Information Office under the amendment provisions of the Privacy Act of 1974, as amended.

23-9. NCIS HQ File Search and Retrieval

a. Documentation concerning investigations and counterintelligence operations

conducted by NCIS personnel world-wide, NCIS employment investigations and security clearance adjudication material created by the DON Central Adjudication Facility (DON CAF) (until January 23, 2013) or appellate authority, and U.S. Navy and Marine Corps Incident Reports (IR), Navy and Marine Corps CID investigations and NCIS Report of Investigation (INFO) (also known as ROI (INFO)) (formerly called NCIS Operations Reports) is ultimately transmitted to NCISHQ RMB for retention as temporary or permanent records as prescribed by reference (d). NCISHQ RMB is charged with the responsibility of ensuring the proper maintenance and availability once these investigations become closed cases. The records are located within the NCIS Records Information Management System (RIMS) or can be obtained from the Washington National Records Center (WNRC) in Suitland, Maryland. This section of the chapter discusses the systems by which information is filed and the methods available to search for and retrieve it. This section also discusses the methods by which authorized personnel may retrieve records from other DoD and non-DoD Federal agencies.

b. Types of Searches. The database contains tracings that can be searched using three different methods:

(1) NAME (also known as PERSON) SEARCH:

(a) The records within this database contain the name and known personal identifying data (PID) (i.e., Social Security number (SSN), date of birth, and or place of birth) of individuals who were investigated or otherwise involved as subjects (S), victims (V), or cross references (CROSS REF or X-Ref) in an investigation, operation, or adjudication action.

(b) The DCII provides two major types of information: investigative agency file tracings and NAC tracings. (Of note, security clearance adjudication tracings are no longer contained in the DCII. This information is now available in the Joint Personnel Adjudication System (JPAS)). A file tracing usually indicates that a dossier (file) on the subject of the search exists. (Tracings for favorable NCIS Counterintelligence Security Polygraph (CSP), i.e., 9PN for Navy and 9PM for Marines, are exceptions. In these cases, there is no dossier; only a DCII tracing that advises that the polygraph was favorable).

(c) Provided in the file tracing is information identifying the contributing agency and the pending (i.e., reflected on the DCII tracing as "open") or closed status of the matter. No investigative information is contained in the tracing.

(d) NAC tracings specify that a given individual has a NAC investigation either pending or completed. The completed NAC reflects the date and specific national agencies checked.

(e) To conduct a search on person tracings, at least one PID element such as the date of birth, place of birth or SSN must be available in addition to the name. If the person has a new (i.e., maiden) name or aliases, they may also have to be searched.

(2) Name Only Search: This database provides users with a means of retrieving information from records containing a name, but no other PID. The record format is otherwise

identical to the PERSON search.

(3) Impersonal Title Search: This database provides users a means of maintaining and retrieving information pertaining to impersonal titles (i.e., organizations and incidents).

c. Obtaining DCII Tracings

(1) The DCII system is available through the world wide web based application that provides access to the full range of DCII system functions. This includes query, add, delete, update, and print of the Person, Name Only, and Title Indices: file demands of the Person Index, query of the Office of Personnel Management (OPM) Security/Suitability Investigations Index (SII) and view/print of reports. This internet address is https://dcii.dmdc.osd.mil /dciiweb/ login/ login.jsp.

(a) Field office personnel can obtain DCII information by submitting requests for checks to their field office during duty hours and to the MTAC Law Enforcement Desk (MTACLE) (b)(6) after NCISHQ duty hours (i.e., from 1530-0600 Eastern Standard Time) or by e-mail at (b)(6) ncis.navy.mil."

(b) In cases where the field offices are unable to access the DCII during NCIS HQ duty hours, they should submit requests to the NCIS HQ RMB Liaison Section, rather than the MTACLE, by calling (b)(6) The Liaison Section will attempt to respond to requests during the same workday.

(2) The DCII online User's Guide contains guidance for conducting the various types of searches. It can be accessed through Lighthouse web page under "Publications\Reference Manuals and User Guides."

d. Search Procedures. In searching for information, one must determine if there is a file pertinent to the investigation or action. A check of the DCII determines if there is a record. During the search process, the computer system selects records with names not conflicting with corresponding elements in the DCII tracing record. If a "NO RECORD" response is received, no further inquiry is necessary.

e. Retrieval Procedures. When the DCII locates a record, the retrieval process will be based on two factors: Requesting Agency and Investigative File Originator

(1) Requesting Agency

(a) If an entity of NCIS is required to retrieve a file located by DCII, a search of the RIM/CRIM systems should be conducted. If the file is located, the file may be retrieved directly by the HQ code or the local field office. Should the file not be located within RIMS/CRIMS, a request should be submitted to RMB requesting assistance in locating the file. Requests can be submitted to (b)(6) @navy.mil".

(b) If an "Other Government Agency" requires an NCIS originated case file located

in DCII, a request should be submitted via the "File Demand" functionality within DCII.

(2) Investigative File Originator. If an entity of NCIS is required to retrieve a file originated by another Government agency located in DCII, a request should be submitted to RMB, via the responsible HQ Code, to order the file. The request should be submitted on NCIS Form 5000.9B.

f. Disclosure Considerations. Prior to disclosure of NCIS HQ investigative file information to outside agencies, the Liaison Section must consider a number of issues, including: The nature and origin of the request, the pertinence of the file information to the inquiry, Freedom of Information and Privacy Acts considerations, the Third Agency Rule, operational priorities, agreements of reciprocity, and the Right to Financial Privacy Act of 1978. For any closed case investigative file released to an agency outside of DoD, a record of disclosure must be filed with the record. All disclosures shall be recorded on OPNAV Form 5211/9 and submitted to NCIS HQ RMB.

23-10. Interpreting DCII Tracings

a. The DCII Users Guide provides explanations for interpreting the various codes used in DCII tracings. Explanations for some of the DCII fields are provided in the following paragraphs:

(1) Case Number. Prior to October 1999, NCIS used a randomly assigned dossier number as the case locator number. This number was separate and distinct from the NCIS assigned case control number. Beginning in October 1999, unclassified cases placed into the RIMS are indexed under the case control number or, for DONCAF cases (until January 23, 2013), the subject's SSN. The case number will be preceded by the letter "C." Cases created prior to October 1999 that are imaged will have their DCII case locator number changed to reflect the case control number. Additionally, cases are no longer commingled. Each case is a separate dossier under its own case control number.

(2) Year Index. Prior to January1, 2000, the year index represented the date the case was opened or the date additional material or cases were added to an existing dossier on a subject. Beginning January 1, 2000, the year index field was changed to represent the year in which the case or action closed. Effective February 4, 2006, DSS updated DCII and created a "Close Date" field. Therefore, the Year Index now represents the date the case is opened.

(3) Open/Closed Case Indicators. Cases, during their pendency, are reflected in the DCII as "OPEN" in the year index field. "OPEN" NCIS cases are masked from the view of non-investigative/adjudicative agency DCII users.

(4) Closed Date. This represents the date the case was closed.

b. Appendix A identifies the most common DCII response field abbreviations. Appendix B identifies file location abbreviations. Appendix C identifies agencies abbreviations. Appendix D identifies place of birth codes.

23-11. Appeals of DCII Index Entries. An individual, or representative of a business entity, who believes he/she, or the business entity represented, was wrongly titled or indexed in the NCIS case management systems (i.e. CLEOC) and the DCII may appeal to obtain a review of the decision.

a. The request for a review must be in writing and addressed to:
Director
Naval Criminal Investigative Service Headquarters
Attn: Code 00L
27130 Telegraph Road
Quantico, VA 22134

b. The requestor must provide an explanation or documentation that established the entry was made due to a mistaken identity or provide a reason(s) why he/she believes that at the time of titling, no credible information existed to indicate that the individual or business committed a crime for which they were titled.

c. Upon receipt of the request, the Director, NCIS will solicit written input from appropriate NCIS staff functions (i.e., Office of Counsel and the Criminal Investigations Directorate). Following review of the staff and counsel opinions, the Director, NCIS will consider the investigative information that was available at the time the initial titling/indexing decision was made.

d. The Director, NCIS, shall notify the requestor in writing of the decision to the appeal. If deciding the individual's or business' identifying information should be removed from the CIS, CMS, or DCII, the Director shall instruct the appropriate staff to make the deletion(s) as soon as practical. If allowing entries to stand, the Director's response to the requestor shall provide information about appellate action, if any.

e. The original request letter, staffing memoranda, and a copy of the response notification will be forwarded to the NCISHQ Head RMB for filing in the applicable case file. The file will be retained for the life of the case file as prescribed by reference (d).

23-12. Assistance. Requests for general assistance may be referred to the RMB DCII Administrator at commercial (b)(6) Requests for assistance on records management issues may be referred to the Head of RMB, at commercial (b)(6) or the Assistant Head RMB, at commercial (b)(6)

APPENDIX A
MOST COMMON DCII RESPONSE FIELD ABBREVIATIONS

ACCESS	Represents current level of access. Clearance information contained in the DCII should not be relied upon. For accurate information, check JPAS.
AGCY	Identifies that made/owns clearance/access entry.
AKA	Also Known As or alias. This refers to other names by which the person is known
CLOSED	Date on which DDIS investigation was closed CASE
CONTEXT	How person is related to file (i.e., subject, victim, x-ref (cross-reference))
CB	Country of birth
DATE INV	Investigation date (i.e., when completed)
DB .	Date of birth, listed by YYYYMMDD
ELIG	Highest level of clearance (or access) eligible for based on type of investigation. Clearance information contained in the DCII should not be relied upon. For accurate information, check JPAS.
FILES	Specifies the investigative files reviewed in conjunction with clearance determination. A "0" indicates no file from that agency was reviewed.
GP	Geopolitical location.
GRANTED	Date associated with issuances, denial, revocation, or suspension of clearance or access or any other action represented by the code entered in the "ELIGIBILITY" data field. Clearance information contained in the DCII should not be relied upon. For accurate information, check JPAS.
LOCATION	Location of the file by agency
NAME	Current name field
NAC	National Agency Check, In DCII, a type of tracing
NAC HIST	Favorable NAC investigation
NAC INC	NAC incomplete
NAC PEND	NAC pending.
NUMBER	File number assigned the case by agency
RETENTION	Number of years to retain file. (Depending on the agency, this could represent the date the case was closed, the date of the most current material in the file, or the date the case was opened.)
SB	State (US) of birth
SSN	Social security number.
TYPE INV	Investigative basis or type of investigation on which the eligibility/access determination is based.
REF	Cross-reference, name/title appears in a file titled under some other name or title

APPENDIX B
FILE LOCATION ABBREVIATIONS

NCIS	Naval Criminal Investigative Service Headquarters
AFOSI	Air Force Office of Special Investigations
ACRD	Army Crime Records Center
AIRR	Army Investigative Records Repository
DDIS/DDISF	Defense Security Service (formerly Defense Investigative Service)
DISX	Defense Security Service Project Cases (formerly Defense Investigative Service Project Cases)
NSA	National Security Agency
DODIG	DoD Inspector General
DISCR	Directorate for Industrial Security Clearance Review
DIA	Defense Intelligence Agency

APPENDIX C
AGENCIES ABBREVIATIONS

1	DCII	Defense Central Index of Investigations
2	FBI-HQ	FBI Headquarters
3	FBI-CRM	FBI Criminal File
4	FBI-T	FBI Ident. Div. Fingerprint Check
4	FBI-N	FBI Ident. Div. Name Check Only
6	TAG-O	Army Military Personnel Center Active Duty (Officer)
7	TAG-E	Army Military Personnel Center Active Duty (Enlisted)
8	AF-MPRD	Air Force Military Personnel Center - Active Duty
9	BUPERS	Navy Military Personnel Records
10	USMC	Marine Corps Personnel Records
11	CG(PRS)	Coast Guard Personnel Records
12	USCG	Coast Guard Personnel Records - Intelligence
13	MPRC	Prior Active Duty Service Records
18	OPM	Office of Personnel Management
19	CIA	Central Intelligence Agency
20	I&NS-C	Immigration and Naturalization Service-Citizen
21	I&NS-A	Immigration and Naturalization Service-Alien
22	STATE-S	Department of State - Security
23	STATE-P	Department of State - Passport
24	STATE-C	Department of State - Birth Abroad of U.S. Citizens
25	FRC	Federal Records Center
26	ARPC	Air Force Reserve Personnel Center
27	SS	U.S. Secret Service
28	IRS	Internal Revenue Service
29	CUSTOMS	U.S. Customs Service
30	DEA	Drug Enforcement Agency
31	ICA	International Communications Agency (formerly U.S. Information Agency)
32	AID	Agency for International Development

APPENDIX D
PLACE OF BIRTH CODES

AL	Alabama
AK	Alaska
AS	American Samoa
AZ	Arizona
AR	Arkansas
CA	California
CO	Colorado
CT	Connecticut
DE	Delaware
DC	District of Columbia
FM	Federated States of Micronesia
FL	Florida
GA	Georgia
GU	Guam
HI	Hawaii
ID	Idaho
IL	Illinois
IN	Indiana
IA	Iowa
KS	Kansas
KY	Kentucky
LA	Louisiana
ME	Maine
MH	Marshall Islands
MD	Maryland
MA	Massachusetts
MI	Michigan
MN	Minnesota
MS	Mississippi
MO	Missouri
MT	Montana
NE	Nebraska
NV	Nevada
NH	New Hampshire
NJ	New Jersey
NM	New Mexico
NY	New York
NC	North Carolina

APPENDIX D (CONTINUED)
PLACE OF BIRTH CODES

ND	North Dakota
MP	Northern Mariana Islands
OH	Ohio
OK	Oklahoma
OR	Oregon
PW	Palau
PA	Pennsylvania
PR	Puerto Rico
RI	Rhode Island
SC	South Carolina
SD	South Dakota
TN	Tennessee
TX	Texas
UM	United States Minor Outlying Islands
UT	Utah
VT	Vermont
VI	Virgin Islands of the United States
VA	Virginia
WA	Washington
WV	West Virginia
WI	Wisconsin
WY	Wyoming

CHAPTER 24A
TITLE: PERFORMANCE MANAGEMENT FOR NCIS EMPLOYEES UNDER THE GENERAL SCHEDULE (GS)
POC: CODE 10A
DATE: SEP 10

REFERENCES:
A. Title 5, USC, Chapter 43
B. 5 CFR, Chapter 430
C. DODI 1400.25, Volume 430
D. DON Civilian Human Resources Manual, Subchapter 430.1
E. DON Civilian Human Resources Manual, Subchapter 432.1
F. DON Civilian Human Resources Manual, Subchapter 351
G. DON issuance governing the Interim Performance Management System Covering Positions Transitioning to the General Schedule from the National Security Personnel System, Ver 1.1, May 2010

24A-1. PURPOSE

This chapter complies with references (a) through (g) and outlines the performance management policies and procedures for Naval Criminal Investigative Service (NCIS) employees covered under the General Schedule (GS).

24A-2. DEFINITIONS

Appendix 1 provides definitions of terms.

24A-3. POLICY

24A-3.1. NCIS will use effective performance management to reward employees in proportion to their contributions to mission, to improve employee performance and organizational effectiveness, and to identify and take corrective action to improve poor performance.

24A-3.2. NCIS will evaluate employee performance using a two-level rating system, defining employee performance as either “acceptable” or “unacceptable.”

24A-3.3. The goal of the performance management system is to involve employees in improving organizational effectiveness by integrating processes that:

a. Communicate and clarify NCIS mission and organizational goals and objectives.

b. Identify employee, team, and supervisory accountability for the accomplishment of goals and objectives, as identified in the critical elements of performance plans.

c. Use appropriate measures of performance to recognize and reward employees and use the results of a performance appraisal as a basis for appropriate personnel actions.

d. Encourage employees to take responsibility to continuously improve, support NCIS priorities and goals, develop professionally and perform at their full potential.

24A-4. SCOPE

This chapter applies to all NCIS employees in grades GS-1 through GS-15.

24A-5. RESPONSIBILITIES

24A-5.1. Director, NCIS

a. Establish and communicate organizational priorities, goals and objectives to guide the NCIS strategic plan and program direction documents, which provide the basis for individual performance goals.

b. Approve the funding level for performance awards.

c. Establish NCIS performance management policies.

d. Oversee the structure and composition of the Performance Award Review Boards (PARBs) and provide guidance to them as required.

24A-5.2. PARB Chairs

a. Distribute performance award funds in a manner consistent with NCIS performance management policies, business rules and fiscal guidance.

b. Ensure performance award decisions are made in a consistent manner and in compliance with Merit System Principles.

c. Ensure the rationale for granting performance awards is fair and equitable across the NCIS organizations under review.

24A-5.3. Senior Rating Officials (SROs)

a. Serve as the final approving official for each employee's rating of record. SROs are responsible and accountable for ensuring the accuracy, consistency and fairness of performance management decisions within the organization(s) for which they are responsible.

b. Ensure subordinate Rating Officials (ROs) are fully trained to carry out their performance management responsibilities.

c. Ensure employees are fully trained in the performance management system.

d. Ensure performance plans are established within required timeframes.

e. Ensure completed ratings of record and recommendations for awards are forwarded to the PARB within required timelines and in accordance with guidance prescribed by NCIS Human Resources Directorate, Personnel Operations and Services Department (Code 10A).

24A-5.4 Rating Officials (ROs)

a. Effectively monitor and assess the performance of their employees.

b. Execute performance management activities in a manner consistent with Merit System Principles.

c. Align performance and employee development plans with the NCIS mission, program goals, and field/headquarters tactical plans, and effectively communicate their expectations to employees and hold them accountable for achieving the desired results.

d. Involve employees in the development of performance plans and ensure that all employees have a copy of their approved performance plan within 30 days of the beginning of each appraisal period and for each detail or temporary promotion expected to last 120 days or longer.

e. Provide meaningful performance feedback to their employees throughout the rating cycle by conducting periodic progress reviews (at a minimum, midway through the annual performance cycle).

f. Prepare close-out ratings as appropriate.

g. Propose a final rating of record and make appropriate recommendations for awards within the timeframes prescribed by Director, NCIS and/or Code 10A.

h. Foster and reward excellent performance.

i. Address poor performance with the assistance of the Employee Relations Specialist, Human Resources Services Division (Code 10A2).

j. Identify and recommend, at the earliest opportunity, separation of trial period employees whose performance or suitability is unacceptable for continued employment.

k. Communicate final ratings of record and award decisions, if any, to each individual employee no later than 75 days after the end of the appraisal period.

24A-5.5. Employees

a. Collaborate with their supervisors to develop critical elements for their performance plans;

b. Develop an understanding of the link between their critical elements and NCIS mission, program goals, and field/headquarters tactical plans.

c. Record accomplishments and results in self assessments for any close-out rating(s), and their final rating of record.

d. Participate in progress reviews and final performance appraisal discussions within the established timeframes. Additionally, employees are strongly encouraged to actively participate in all phases of the performance management cycle.

e. Serve a two-year trial period upon appointment as a special agent or a one-year trial period upon appointment to any other position. Additionally, employees newly appointed to a supervisory position will serve a one-year supervisory probationary period.

24A-5.6. NCIS Code 10

a. Provide procedural information to managers and employees regarding the performance management process.

b. Manage the timeliness of the performance management process.

c. Validate employee and rating data before and after the NCIS PARB process.

d. Provide assistance to the PARB Chairs to ensure the requirements of this chapter are fully met and that resulting reports and personnel actions are appropriately completed and processed.

24A-6. PERFORMANCE APPRAISAL REQUIREMENTS

24A-6.1. Appraisal Period

a. An annual appraisal period is required for rating of record purposes. The annual appraisal period commences on 1 October and concludes on 30 September of the following year.

b. To receive a rating of record, an employee must have served for a minimum appraisal period of 90 days under an approved performance plan in the same position. If necessary, the employee's appraisal period may be extended beyond 30 September by the RO with approval from the SRO to insure the minimum 90 day period is met. Approvals for extension, however, cannot interfere with the NCIS rating and rewarding calendar. For example, an RO could extend the appraisal period until 10 October for an employee who transferred to the new field office on 10 July since this would still permit the employee to complete his/her self assessment and the RO to complete his/her assessment/recommended rating of record in sufficient time to receive SRO review and approval by the stated deadline (e.g., 15 November).

c. When the appraisal period cannot be extended so that an employee can perform for a minimum 90-day requirement under an approved performance plan (e.g., an employee who transfers to a new position after the end of July) the close-out rating from the previous position will serve as the rating of record. Any remaining period of time within the appraisal period is added to the following year's annual appraisal period.

24A-6.2. Performance Plans

a. In accordance with reference (c), no employee may be concurrently covered by more than one performance appraisal system. A special agent enrolled in the Special Agent Basic Training Program or covered by the Field Training Evaluation Program must be covered by a performance plan under this chapter.

b. Each employee must have an approved written performance plan based on work assignments and responsibilities. Only the DON Interim Performance Appraisal Form June 2010 may be used for the creation of performance plans and appraisal/rating of performance.

(1) SROs must approve each employee's performance plan. The employee, the RO and the SRO are required to sign and date the performance plan in Part B of the DON Interim Performance Appraisal Form June 2010. The employee's signature acknowledges only that the plan has been communicated to the employee.

(2) Employees must receive a copy of their approved, signed performance plans no later than 30 days after the beginning of the rating period, permanent assignment to a new position, and for each detail, temporary assignment or promotion expected to last more than 120 days. Performance plans must include all critical elements and related performance standards. Failure to meet this requirement is grievable (see 24A-8b).

c. At the time the performance plan is established, the RO must certify if the employee's position description (PD) is accurate. If the PD is not accurate, the RO must take corrective action to update the PD with the assistance of the Position Classification Specialist, HR Operations Division, Code 10A1.

d. Critical Elements

(1) Each performance plan should have a minimum of two, but generally between three and five, critical elements that address individual employee objectives and expectations. Critical elements are derived from an employee's work assignments, and must be clearly aligned to NCIS priorities, program plans and Field Office/HQ tactical plans.

(2) A critical element must be sufficiently specific so as to be understandable by the employee and assessable by the RO and should be comprehensive enough to span the entire rating period. Critical elements must be commensurate with the employee's grade, career status (e.g., entry, journey, or senior/expert level), experience in the position and the requirements of the position itself. Critical elements may not be weighted.

(3) Performance plans for supervisors must contain at least one supervisory critical element. An NCIS standard supervisory/managerial critical element will be published in advance of the start of each appraisal period and will be required to be included in the performance plan of all supervisors.

(4) Certain positions also have requirements for specific areas of responsibility (e.g., safety, security, acquisition). Establishment of specific critical elements may not be necessary in all instances. Rather, it may be appropriate to combine these expectations into one or more job-specific critical elements. Reference (g) contains further guidance.

(5) NCIS may establish standard critical elements for identified positions. Any standard critical elements established by NCIS will be published in advance of the start of each appraisal period, or at a minimum, in time to provide a performance period of at least 90 days prior to the end of the rating period. ROs are required to include standard critical elements identified as mandatory in the performance plans of the identified positions.

e. Performance Standards

(1) Each critical element is measured by DON-defined performance standards, which are an expression of the performance thresholds, requirements, or expectations that must be met to be appraised at a particular level of performance.

(2) DON has defined critical element performance standards at three career stages (entry, journey, and expert) both at the "unacceptable" level and the "acceptable" level. Additionally, DON has defined a critical element performance standard to be used for all supervisors. The DON Critical Element Performance Standards are contained in Appendix 2.

24A-6.3. Monitoring Performance. Throughout the rating cycle, ROs and employees will monitor performance to ensure the performance plan continues to accurately reflect job requirements and organizational priorities. Critical elements may be modified, added to, or deleted from employee performance plans as needed throughout the performance period.

a. Adjusting Critical Elements

(1) Reasons for adjusting critical elements include:

(a) Conditions that change beyond the employee's ability to control or influence;

(b) Complexity of the job/performance objective(s), or the associated resources to complete the objective were underestimated; or,

(c) Changes in staffing, organizational structure, priorities, etc.

(d) Assignment of new responsibilities or projects.

(2) There is no required minimum period of time an employee must be under notice of an adjusted critical element, except that a critical element cannot be assigned or adjusted within 90 days of the end of the appraisal period and it must be achievable during the remaining portion of the appraisal period.

(3) Adjustments to critical elements must be communicated to the employee after having been approved by the SRO.

b. Conducting Progress Reviews

(1) While ongoing informal dialogue and feedback are essential throughout the appraisal period, one midyear progress review is required, at which time employees must be informed of how they are progressing with regard to their critical elements.

(2) The required progress review is documented in Parts E, F and G of the DON Interim Performance Appraisal Form June 2010. An additional progress review may be documented to support effective performance monitoring using Parts H, I and J of the DON Interim Performance Appraisal Form June 2010.

(3) The progress review should discuss achievements to date against critical elements and identify areas where improvement is needed, and provide meaningful dialogue and exchange of concerns. Developmental suggestions also may be provided to the employee, as appropriate.

(4) To the extent possible, the progress review will be conducted as part of a face-to-face discussion. Other means such as teleconference or video-teleconference are allowed where unusual circumstances (such as geographic separation) dictate.

(5) The assignment of a summary rating by ROs is not appropriate during these reviews.

(6) Employees are expected to submit a midyear progress narrative assessment, referred to as a self-assessment. This narrative self assessment is documented in Part E of the DON Interim Performance Appraisal Form June 2010.

(7) Rating Officials will provide a written assessment for the progress review. The RO assessment is documented in Part F of DON Interim Performance Appraisal Form June 2010.

(8) ROs, SROs, and employees sign and date the performance plan form in Part G of the DON Interim Performance Appraisal Form June 2010 to indicate that the progress review was conducted. Failure by an employee to sign does not void the content of the performance plan or progress review.

24A-6.4. Closeout Ratings

a. A closeout rating is a narrative description of an eligible employee's performance under established critical elements, and is completed by the RO to convey information regarding the employee's progress toward the completion of the critical elements. Closeout ratings are documented in Parts K and L of the DON Interim Performance Appraisal Form June 2010.

b. Closeout ratings are required when:

(1) An employee completes a detail or a temporary promotion of more than 120 days under established critical elements.

(2) An employee changes positions, is promoted or leaves NCIS after being under established critical elements for a minimum of 90 days.

(3) The RO leaves the position after the employee is under established critical elements for a minimum of 90 days. In this situation, the employee may continue under the same performance plan unless it is changed by the new RO.

(4) Acting ROs are required to complete closeout ratings for any employee they have supervised for periods of 90 days or more.

b. Closeout ratings may become the rating of record if there is insufficient time (fewer than 90 days) to establish a new performance plan and rate the covered employee in the newly assigned position before the end of the rating period.

c. Closeout ratings will be accomplished in a timely manner and will be considered by the appropriate RO when determining the employee's recommended rating of record and any recommendations for awards at the end of the appraisal period.

24A-6.5. Rating of Record and Summary Level Rating. The rating of record is prepared at the end of the appraisal period and includes assignment of a summary level rating: "acceptable" or "unacceptable." This performance appraisal consists of an employee self assessmentand RO assessment of performance on each critical element, documented in Part N of the DON Interim Performance Appraisal Form June 2010.

a. Employee Self-Assessments. Employees are required to provide a written narrative for each critical element covering their performance and contributions for the current appraisal

period. Employee self-assessments will describe accomplishments relative to performance expectations, including critical elements, associated performance standards, and contributions to the NCIS mission, program direction and/or field office/HQ office goals, etc. The employee's self assessment will assist the RO in evaluating more fully the employee's performance results. The employee's perspective will better inform the RO of performance and contributions, and thereby may impact the recommended rating and any award recommendations. To facilitate completion of this self-assessment, employees are encouraged to maintain a personal record of their accomplishments, achievements, and performance throughout the appraisal period.

b. RO Assessment. The RO assessment captures the employee's accomplishments, or lack thereof, where applicable, during the appraisal period. The first step is to evaluate employee's performance relative to the critical elements when compared with the performance standards. An individual element level rating of either "acceptable" or "unacceptable" must be assigned to each critical element. Individual element level ratings are then converted to one of two summary level ratings: "unacceptable" as the lowest and "acceptable" as the highest. An "unacceptable" summary level rating for the appraisal period is assigned if performance in one or more critical elements is rated as "unacceptable."

c. Completing and recording the results. ROs must complete employee assessments within 30 days of the end of the appraisal period. ROs are required to have a conversation with their employees to discuss the rating of record, the RO narrative assessment, as well as any recognition/rewards within 75 days of the end of the annual appraisal period. This conversation may occur only after the SRO review and approval of the rating of record, and approval by the PARB of any award recommendation. Employees must be provided a copy of their rating of record and RO narrative assessment. Employees will be required to sign the rating of record to indicate that they have received the rating. The employee's signature does not necessarily indicate agreement. Annual appraisal signatures are recorded in Part P of the DON Interim Performance Appraisal Form June 2010.

24A-7. UNACCEPTABLE PERFORMANCE

24A-7.1 Taking Action on Unacceptable Performance

a. If an employee's performance is determined to be "unacceptable" in one or more critical elements at any time during the appraisal period, the rating official must take corrective action by speaking with the employee about the performance issue and suggesting ways to improve performance.

b. Should the unacceptable performance continue, the rating official must contact Code 10A2 immediately for guidance prior to formally notifying the employee in writing with a "Notice of Unacceptable Performance." This notice must include:

(1) An identification of which critical element(s) have been deemed "unacceptable."

(2) The performance requirement(s) and standards that must be attained to demonstrate acceptable performance.

(3) A reasonable opportunity period in which to demonstrate acceptable performance.

(4) Assistance in improving performance, which may include formal training, on-the-job training, counseling, closer supervision, or other appropriate measures.

c. A rating of record of “unacceptable” may not be assigned until the Notice of Unacceptable Performance has been provided to the employee and the opportunity period identified in the notice has passed without improved and sustained acceptable performance. Should this occur, at a minimum, the RO must either deny or delay any within grade step increase. Additionally, the RO may initiate reassignment. Reduction in grade or removal may be initiated only after a formal performance improvement plan (PIP) has not been successfully completed.

24A-7.2. A rating of record of "unacceptable" must be reviewed and approved by the SRO.

24A-7.3 Withholding A Within Grade Increase (WGI)

a. A WGI is to be withheld from an employee who receives an “unacceptable” rating of record. The affected employee must be given a written notice of the intention to withhold the WGI within 30 days following the end of the waiting period or other period upon which the negative determination is based. This notice must include the following:

(1) The reasons for the negative determination to include specific critical elements that the employee is not performing acceptably and the performance standard necessary to support the granting of the WGI.

(2) Instructions to the employee on the right to request reconsideration in writing within 15 calendar days after receiving the notice.

(3) The name of the deciding official to whom the request for reconsideration is to be submitted.

b. The affected employee has the right to:

(1) Be advised by a representative of his/her own choosing. The deciding official may disallow the choice of an individual as a representative if that choice would result in a conflict or apparent conflict of interest or position, a conflict with the priority needs of NCIS, or unreasonable cost.

(2) Review the file containing all of the information the deciding official will use to make a determination.

c. Based on the information provided by the supervisor and the employee, if provided, the deciding official may reverse or sustain the negative determination.

d. ROs, SROs, and deciding officials must insure close liaison with Code 10A2 before and during the process of withholding a WGI.

24A-8. GRIEVANCES AND APPEALS

Employees who disagree with their summary level rating/rating of record should first attempt to resolve the issue through discussion with their immediate supervisor. If this step fails to resolve the issue to the employee's satisfaction, the employee may grieve the issue through the administrative grievance procedures (see NCIS-1, Chapter 17, Administrative Grievance System). Guidance on grievable/appealable matters is as follows:

a. The substance of an employee's critical elements is not grievable.

b. Failure to inform employees of critical elements and performance standards within the required time frame is grievable.

c. Ratings on individual critical elements and summary level ratings are grievable.

d. Performance-based demotions and removals may be appealed to the Merit Systems Protection Board (MSPB).

e. Receipt or non-receipt of a performance award or other recognition is not grievable.

24A-9. PERFORMANCE RECOGNITION

To recognize and reward employees based on their accomplishments and contributions, each critical element assigned a rating of "acceptable" is also assigned a reward recommendation score of 1, 2 or 3. The performance standards used for reward recommendations are contained in Appendix 2. The average of the reward recommendation scores at the individual critical element level will form the basis for overall reward recommendation and eligibility.

a. Awards are tools to acknowledge and motivate employees by recognizing and rewarding significant individual and team achievements and contributions. Performance award amounts are expressed as a percentage of basic pay. Performance awards are neither mandatory nor guaranteed. The awards amounts for the FY 2010 and subsequent performance cycles will be published as they become available.

b. When determining an award amount, ROs and SROs should consider other recognition received by employees during the appraisal period. Similarly situated (career stage, position, responsibilities, critical elements) employees with like performance should be rewarded in a consistent manner. SROs and PARBs will ensure that there are clear distinctions in award amounts for different levels of performance and contribution to mission.

c. After the SRO has approved award amounts for each employee, the PARB will approve or disapprove the recommendations to ensure fairness, consistency and adherence to Merit System

Principles and appropriateness in light of NCIS business decisions. NCIS-wide business rules for PARBs will be followed to ensure consistency across the agency.

APPENDIX A – DEFINITIONS FOR KEY PERFORMANCE MANAGEMENT TERMS

Acceptable Performance. Performance that meets an employee's performance requirement(s) or standard(s) at a level of performance above 'unacceptable' in the critical element(s) at issue

Activity (or Organization). A Department of the Navy (DON) field installation, Headquarters command or Headquarters office.

Appraisal. The process under which performance is reviewed and evaluated against the described performance standard(s).

Appraisal Period. The established period of time for which performance will be reviewed and a rating of record prepared.

Award. Recognition for individual or team achievement that contributes to meeting organizational goals or improving the efficiency, effectiveness and economy of the government or which is otherwise in the public interest.

Close-out Appraisal. An appraisal conducted when an employee or first-level supervisor leaves a position or ceases to have rating responsibilities after the employee has been under established performance standards for at least 90 days or more but before the end of the appraisal period. Close-out ratings will be documented and used in deriving the rating of record and, in some cases, may become the rating of record.

Critical Element. A work assignment, goal, objective or responsibility of such importance that unacceptable performance on the element would result in a determination that an employee's overall performance is unacceptable.

Day. Unless otherwise specified, calendar day.

Individual Element Level. The assessment of accomplishment and contribution to mission for each critical element in a performance plan as measured against performance standards.

Performance. Accomplishment of work assignments or responsibilities.

Performance Plan. All of the critical elements and their selected performance standards that describe the expected performance of an individual employee.

Performance Awards Review Board. A group of senior leaders of an organization whose responsibility it is to review and approve all performance awards at a strategic level for fairness, appropriateness and adherence to Merit System Principles.

Performance Standard. The DON-approved expression of the performance threshold(s), requirement(s) or expectation(s) that must be met to be appraised at a particular level of performance. A performance standard may include, but is not limited to, quality, quantity, timeliness and manner of performance.

Position Description. Officially documents management's assignment of major duties, responsibilities and organizational relationships to a position. Because it serves as the official record of the classification of the job, it can be used to make other personnel decisions, such as deriving critical elements.

Progress Review. One or more required conversations with an employee about performance as it relates to critical elements measured against applicable performance standards.

Rating of Record (also 'Summary Level'). The performance rating prepared at the end of an appraisal period for performance over the entire period including the assignment of a summary level. The Rating of Record is the official rating for pay and retention purposes.

Rating Official. A rating official, generally an employee's first-line supervisor, is responsible for establishing performance plans for his/her employees based upon the parameters identified in this policy, carrying out required performance reviews with employees, taking action as necessary to correct less than satisfactory performance, and recommending a Summary Level and Rewards Recognition for performance (as appropriate) to the senior rating official. The rating official must be a management official as described in reference (b) and is typically the immediate supervisor.

Reward Recommendation. A method for distinguishing between employees for purposes of determining awards eligibility.

Senior Rating Official. Generally, the senior rating official is an employee's second-line supervisor, and is responsible for reviewing and approving performance plans, recommended ratings of record, close-out ratings and rewards and recognition to ensure consistency and fairness within and across parts of an organization within that individual's span of control.

Summary Level (also 'Rating of Record'). The final result of the performance appraisal process. The summary level is used to provide consistency in describing ratings of record. The two summary levels are 'acceptable' and 'unacceptable'.

Unacceptable Performance. Performance of an employee that fails to meet established performance standards in one or more critical elements.

Pages 509 through 518 redacted for the following reasons:
- -
(b)(5)

CHAPTER 25 – SECTION 1
TITLE: SSD REPORT WRITING
POC: CODE 11C
DATE: JAN 10

APPENDICES
(1) PRODUCTION AREAS, CASE CATEGORY LIST AND DEFINITIONS

POLICY DOCUMENTS
APPENDIX (2) Gen Admin 11C-0016 of 19 May 2011 released NCIS Policy Document No 11-07 Administrative (9Y Project Code Identifiers in NCIS Manuals). Policy document 11-07 contains revised or new policy that has not been incorporated into this chapter and should be reviewed in its entirety.

APPENDIX (3) Gen Admin 11C-0019 of 02 Jun 2011 released NCIS Policy Document No. 11-10 Operational (Expanded Reporting Requirements For Sexual Assault Investigations). Policy document 11-10 contains revised or new policy that has not been incorporated into this chapter and should be reviewed in its entirety.

ADDENDUMS

SAMPLES

(27) SAMPLE PRESENTATION SUMMARY

25.1-1. PURPOSE

a. The majority of reports prepared by the Naval Criminal Investigative Service (NCIS) serve to document investigative effort. The NCIS documentation system follows requirements necessary to document the results of criminal investigations to assist the appropriate federal, state and/or military criminal justice authorities in adjudicating allegations of criminality. A secondary purpose of the report system is to provide information necessary to fulfill a variety of administrative requirements within NCIS and Department of the Navy.

b. This chapter addresses policy, procedures, and guidance concerning the use and preparation of NCIS SSD documents for reporting investigative and non-investigative information. Policy, procedures, and guidance concerning the use of the Department of the Navy Criminal Justice Information System (DONCJIS) for unclassified criminal investigations are found in NCIS-1, Chapter 25.2, DONCJIS Report Writing. Related policy, procedures, and guidance for DONCJIS system management (e.g., user accounts, roles) can be found in NCIS-1, Chapter 25.3, DONCJIS System Management.

c. This chapter will not address reporting requirements associated with the NCIS Central Source Registry (CSR) or classification guidelines. CSR protocol is found in NCIS-3, Chapter 8 (available via SIPRnet) and classification guidelines are found in the Department of the Navy Information Security Program (ISP) Regulation 5510.36, Chapters 4 (Classification Management) and 6 (Markings). Additionally, information pertaining to CI or CT operations reporting is addressed in NCIS-4.

25.1-2. KEY TERMS

25.1-2.1. Control Office. NCIS component that initiates an investigation or operation. Includes a NCIS component that assumes responsibility for an investigation or operation when control is transferred to it by another NCIS component.

25.1-2.2. Control Agent (Case Agent). Individual who is tasked with primary investigative authority and responsibility for the case. The case will be listed under this person's name in the NCIS Case Control System 2000 (CCS).

25.1-2.3. Lead Office. NCIS component, other than the control office, tasked by Report of Investigation (ROI) (ACTION) to perform investigative or administrative action(s) in connection with an investigation.

25.1-2.4. Participants. Any individual who actively assists in the actual conduct of an investigation or inquiry.

25.1-3. RESPONSIBILITIES

25.1-3.1. Management. It is the responsibility of each field manager and supervisor, i.e., NCIS Special Agent in Charge (SAC), Assistant Special Agent in Charge (ASAC), and Supervisory Special Agent (SSA), to ensure quality review procedures are in place to validate timeliness, accuracy, and completeness of investigative data and reports. For further information, see NCIS-1, Chapter 45, which describes and assigns responsibility for management processes that are necessary to maintain the quality of NCIS' investigative and operational activities.

25.1-3.2. Control Agent. It is the responsibility of each Special Agent (SA) assigned as control agent (case agent) to enter investigative data into applicable NCIS reporting systems, from initiation through closure of an investigation or inquiry, and to ensure all data is complete, accurate and to produce a timely investigative product in accordance with NCIS policy and procedures.

25.1-3.3. Lead Agent. It is the responsibility of the agent receiving lead tasking from another NCIS office to respond according to timeliness requirements set forth in 25.1-9.

25.1-3.4. Participants. It is the responsibility of each NCIS employee assigned as a participant on an investigation to provide timely, accurate, and complete investigative data and documents to the case control agent.

25.1-4. STANDARD SYSTEM DOCUMENT (SSD)

25.1-4.1. The NCIS Standard System Document (SSD) is a multi-purpose format used for various reporting requirements. SSDs are used to transmit information among NCIS components by mail and NCIS networks. SSD format is also used in the text of Naval Messages when that form of communication is required. There are three (3) SSD types utilized to meet investigative, operational, and administrative needs. Regardless of the SSD type, the text will be prepared in upper and lower case letters. The last name of any named person is required to be in UPPER CASE. When Naval Messages are used for transmission, UPPER CASE text is required.

25.1-4.2. Header/Footer Requirements. All paper copy investigative/operational reports submitted to NCISHQ for record purposes or disseminated to entities outside of NCIS will bear the following computer-generated "header and footer" caveats on all pages of the documents.

a. Header: **U.S. NAVAL CRIMINAL INVESTIGATIVE SERVICE** in bold, top of each page of the document, left margin justified.

b. Footer: Classification level of the document. For unclassified documents generated on the NCIS Report Writing system, the classification level will be defaulted to "**FOR OFFICIAL USE ONLY**". Each page of the document will bear page markings and the initials of the releasing official on the last page of the document. The page markings/releasing official initials will appear directly beneath the classification marking.

c. Overall classification must be conspicuously placed at the top and bottom of all classified documents.

d. Each page of the document will contain the "Warning" caveat on the bottom right of the page;

WARNING

THIS DOCUMENT IS THE PROPERTY OF THE NAVAL CRIMINAL INVESTIGATIVE SERVICE. CONTENTS MAY BE DISCLOSED ONLY TO PERSONS WHOSE OFFICIAL DUTIES REQUIRE ACCESS HERETO. CONTENTS MAY NOT BE DISCLOSED TO THE PARTY(S) CONCERNED WITHOUT SPECIFIC AUTHORIZATION FROM THE NAVAL CRIMINAL INVESTIGATIVE SERVICE.

e. Paper copy classified documents (i.e., "Confidential," "Secret," etc.) will use the same header and footer requirements as for unclassified documents, but will contain appropriate paragraph classification levels, overall classification of the document, classification authority and declassification instructions.

25.1-4.3. SSD Types

a. General Administration (Gen Admin). Gen Admins are used to document administrative and policy matters, and are not authorized for operations, investigative tasking, or reporting. A Gen Admin may be utilized by NCISHQ to communicate a directive or administrative request for information to NCIS field components. When utilized to request information, the Gen Admin will document in the final paragraph a synopsis concerning the information being requested, date of completion and where requested information should be directed. Format of Gen Admins differs significantly from other NCIS SSD documents in that they are drafted in memorandum format. Sample (1) is a Gen Admin that requests information and Sample (2) is a Policy Gen Admin example. Only NCIS Headquarters is authorized to prepare Policy Gen Admins, which are coordinated with the Administrative Services Department (Code 11C) and require approval of the Director (0000). SSD document numbers are assigned by the respective NCISHQ code preparing the Gen Admin, and each NCISHQ directorate or department will maintain a log of sequential Gen Admin control numbers. On the "FROM" line, SSD document numbers are placed on the right side justified. Document numbers reflect the code preparing the Gen Admin followed by a hyphen, and the next sequential number of the calendar year (i.e., 22-0001, 22-0002). The code-office designator within the Gen Admin number field is limited to a maximum of four characters. Policy Gen Admin documents have a structured title format. Administrative Services Department assigns policy document numbers, which are placed in the title when release is approved. Policy Gen Admin numbers consist of two-digit numbers of the calendar year followed by a hyphen and then the next sequential group consisting of four (4) numeric entries, beginning with 0001 and continuing to 9999. Sequence numbers will be restarted at the beginning of every calendar year (07-0001, 08-0001, 09-0001, etc.).

(1) As part of the Policy Gen Admin, the document title will be an identifier, which advises the reader of the topical area of the document. Authorized topical areas are:

ADMINISTRATIVE
OPERATIONAL
PERSONNEL
LEGAL MATTERS

TRAINING
INFORMATION MANAGEMENT

(2) Following the topical area, the specific area being addressed is set in parenthesis. An example of a Policy Gen Admin title is:

SUBJ: NCIS POLICY DOCUMENT NO. 08-0038: LEGAL MATTERS (PRIVACY ACT VIOLATIONS)

b. Investigative Action (IA). IAs are used to formally document all investigative actions during an investigation as accomplished by the control office and lead components, see Sample (3). IAs will be electronically transmitted and subsequently stored in the Case Information System (CIS) as SSDs or in the Case Management System (CMS).

NOTE: IAs DO NOT have a STATUS nor are IAs given an Exhibit number until used as an Exhibit with the appropriate REPORT OF INVESTIGATION (ROI). Even though an IA is electronically transmitted, it cannot stand alone, as does the ROI. If an IA satisfies a lead tasking, it still must be linked to an ROI (ACTION), which responds to completion of the task. The IA is intended for external agency dissemination. Section 25.1-15.2. provides guidance pertaining to the sequential numbering of exhibits reported in a ROI (INTERIM).

EXCEPTION: The following types of investigative reporting will NOT be transmitted electronically via the SSD system: (1) DSI/SI Category 3 and 5 reports; (2) IAs that include restricted access information (Grand Jury, Qui Tam suit, etc.); and (3) Internal Personnel Investigations (Category 2B). NCIS-1, Chapter 5 (Inspector General Matters) provides further guidance on IPI reporting procedures.

(1) Interviews eliciting substantive information from the interviewee should be reduced to a signed sworn statement consistent with the procedures outlined in NCIS-3, Chapter 6 (Investigative Theory and Procedure). This procedure should be followed except in cases where the sworn statements are not desired (e.g., joint/concurrent investigations with other Federal law enforcement agencies and/or U.S. Attorneys, etc.). When an interview is not reduced to a sworn statement, it must be documented in an IA.

(2) Persons interviewed in connection with an investigation will be fully identified in either a statement or an IA. At a minimum, the person's full SSN and/or DOB must be contained within the IA when reporting the results of witness interviews. To help safeguard Victim(s) and Witness(es), the home address and telephone number should not be listed in the IA or statement, but, should be kept in the case file and available to prosecuting authorities. For additional information regarding the Victim and Witness Assistance Program, refer to NCIS-3, Chapter 6 (Investigative Theory and Procedure).

(3) Electronic Transmission of IAs. IAs will be submitted electronically. All IAs completed within a reporting period will be submitted concurrently with the submission of the subsequent ROI.

(4) Timeliness Requirements. IAs should be completed within five (5) business days of the reported investigative activity.

c. Report of Investigation (ROI). The primary Report Writing SSD investigative reporting document. The following identifies the various status types of the ROI and purpose. Sample (4), Sample (5), and Sample (6) show what captions can be found on the ROI template based upon its status.

25.1-5. ROI REPORT TYPES. ROIs with status codes of (OPEN), (ROPEN), (ACTION), (CHANGE), (INTERIM), (CLOSED), (DISP), and (SUPP) are used to report factual information developed during the investigation or operation, and to report completed investigative findings. The (INFO) status code is utilized solely for documenting collected information and passing this on as deemed appropriate.

NOTE: The following case categories are exempt from ROI reporting: 5C (Force Protection Support) and 9Z (Briefings). For reporting guidelines of case category 5C, see NCIS-3, Chapter 38 (Combating Terrorism Investigations and Operations). For reporting results of case category 9Z, utilize the input screen for briefs found on the NCIS Infoweb home page. Click on "Web Applications" then click on the wCIS Brief Application. This is for non-Navy Marine Corps Intranet (NMCI) users only. NMCI users should access wCIS through Citrix.

25.1-5.1. ROI (INFO)

a. Used to report opportunity collection of information involving General Criminal Intelligence (CR), Counterintelligence (CI), Counterterrorism (CT), and Domestic Security (DS) matters. The ROI will NOT be used to report general administrative information or transmit policy. The ROI can be disseminated outside NCIS channels unless it discloses sensitive sources or methods. For an example of an ROI (INFO), refer to Sample (7). In ROI (INFO), the command and UIC line are not required.

b. Used to alert a command to information gained on an opportunity basis, which could affect the security, good order and discipline in the command and not on matters of national level intelligence or high-level interest. When such information is developed, whether of a criminal intelligence nature (i.e., international narcotics production and trafficking) or foreign intelligence/counterintelligence, an Intelligence Information Report (IIR) should be prepared. Detailed guidance on the preparation of an IIR is contained in the Defense Intelligence Agency Manual (DIAM) 58-12, which is accessible through the Defense Intelligence Agency's (DIA) home page on the SIPRNet.

c. The only authorized task that may be forwarded on ROI (INFO) is a request to provide the information to an appropriate organization or official external to NCIS. If a reply to the task is required, respond by ROI (INFO), using the same Title/CCN/Date, and reference the initial ROI (INFO) if an investigation is not initiated. If an investigation is initiated based on information provided in the ROI (INFO), the office receiving the ROI (INFO) will initiate a case using ROI with the status code of (OPEN). The ROI (OPEN) will reference the title, the CCN utilized in the ROI (INFO), and date. When a request is made to apprise a command or a law enforcement agency with the information contained in the ROI (INFO), the originating NCIS office will track

the ROI (INFO). If an investigation or operation is opened by another field component based on the information in the ROI (INFO), the field component opening the investigation must include the originating office that wrote the ROI (INFO) on distribution of the ROI (OPEN) and reference the ROI (INFO).

d. ROI (INFO) will NOT be used to document a complaint/incident, which falls within NCIS jurisdiction but does not result in an open investigation. The complaint/incident will be documented by the ROI (CLOSED) ONLY Report, see Section 25.1-5.7c. It is mandatory to mail ALL ROI (INFO) Reports to the NCISHQ Records Management Branch (RMB) with the appropriate Records Information Management System (RIMS) cover sheet. ROI (INFO) for Death Investigations will be mailed to Code 23 vice the RMB.

25.1-5.2. ROI (OPEN)

a. Will report the receipt of information, which serves to predicate the initiation of the investigation when the information appears credible, NCIS has jurisdiction and the control office has investigative responsibility. An ROI (OPEN) is also used to initiate and control counterintelligence, counterterrorism, and criminal initiative operations. For an example of a ROI (OPEN), please refer to Sample (8).

NOTE: Primarily for internal agency reporting purposes. See Section 25.1-25.2 for dissemination of NCIS SSD reports.

b. The first paragraph of the Narrative portion should clearly state the reason for case initiation; i.e., reactive, reciprocal, details, and disposition, and if applicable, contain the relevant statute(s) that is/are suspected to have been violated.

c. The ROI (OPEN) should answer, at minimum; who, what, where, when, why and/or how the offense was committed. In incidents involving theft or destruction of government property, an estimated value of the item(s) involved should be included when possible.

d. Records Check. When a NCIS investigation is initiated, it is the responsibility of the controlling field office to conduct complete records check of all subjects, co-subjects, and victims. The following database checks for titled subject(s) are the minimum standard for all investigative categories:

(1) National Crime Information Center (NCIC)

(2) Defense Central Index of Investigations (DCII)

(3) Joint Personnel Adjudication System (JPAS)

(4) Consolidated Law Enforcement Operations Center (CLEOC)

(5) Law Enforcement Information Exchange (LINX - where available)

(6) Knowledge Network (K-NET - NIPRNET only)

For investigations that are determined to be Director Special Interest (DSI) cases, the additional database checks K-NET (SIPRNET) and International Justice & Safety Network (NLETS - the state law enforcement database where the subject is a current resident) are mandatory. These database checks should be conducted at the earliest stage in an investigation with their results reflected in the ROI (OPEN).

e. Security Clearance. Place Code 024A (Department of Navy Central Adjudication Facility – DoNCAF) under the INFO distribution section of the ROI (OPEN) if the subject and/or co-subject has a security clearance. In the NCIS Report Writing, the "ELECTRICAL DISTRIBUTION" for Code 024A (DoNCAF) is /24A/.

25.1-5.3. ROI (ROPEN)

a. Used by a NCISFO or NCISHQ control office to reopen a closed investigation. If additional investigative effort is identified after an investigation is closed, the investigation will be reopened by submission of an ROI with the status code of (ROPEN). The ROPEN will list and reference the former title entry, if different. For instance, if a Generic-titled case was closed and new information prompted a reopening of the investigation by Personal title, such as Subject, the ROI (ROPEN) will list the Personal title and reference the Generic title. There will be no need for an ROI (CHANGE) to effect this title change when an ROI (ROPEN) is submitted. The investigation must be reopened with the same case control number (CCN) as that under which it was closed.

NOTE: The ROI (ROPEN) is primarily used for internal agency reporting purposes.

b. Security Clearance. Place Code 024A under the INFO distribution section of the ROI (ROPEN) if the subject and/or co-subject has a security clearance. In the NCIS Report Writing, the "ELECTRICAL DISTRIBUTION" for Code 024A (DoNCAF) is /24A/.

25.1-5.4. ROI (ACTION)

a. Used to request assistance from another office and to report the results of that effort by the tasked office. The purpose code on an ROI (ACTION) will be an "R," which will signify a response is required via an ROI. The format as shown below is "R" followed by a period, then the four-character office code(s) followed by a colon and a narrative statement of the action to be taken. For additional guidance, see Section 25.1-23. For an example of an ROI (ACTION), please refer to Sample (9).

NOTE: The ROI (ACTION) is primarily used for internal agency tasking.

EXAMPLE: ACTION
R. NWBR: Conduct Interview of John JONES.

c. When the tasked office responds to a lead by ROI (ACTION) and the investigation has multiple titles (master title with secondary titles), the responding office is authorized to use the master title with (ET AL) entered after the first line entry of the master title, following example:

S/SMITH, JOHN ARTHUR/YN2 USN (ET AL)
M/W/NEE5/S/123-45-6789/16OCT62/SNOW, ME

NOTE: The use of (ET AL) is authorized only for ROI (ACTIONs) and no other ROI types.

25.1-5.5. ROI (CHANGE)

a. Used when substantive changes to the priority, case category, control number, title block, command line, and/or UIC are necessary during the investigation. The ROI (CHANGE) is primarily used for internal agency reporting purposes. Whenever an ROI (CHANGE) is submitted, it must list the master and all secondary titles for the investigation and should specify exactly what information is being changed or corrected. Any lead offices with the old or incorrect data must be sent a copy of the ROI (CHANGE). Changes should be submitted at the time the new or correct information is obtained. "Corrected Copy" SSD documentation should NEVER be prepared in lieu of an ROI (CHANGE) and "Corrected Copy" should never be typed on an SSD. For an example of an ROI (CHANGE) with ACTION line, please refer to Sample (10). A revised ROI and/or IA should not be transmitted when an ROI (CHANGE) is appropriate. Please refer to Section 25.1-24. for guidance in relation to the Corrective Action Process which must be followed to address certain errors contained in SSDs.

b. Title and CCN Changes. Title information is the means by which NCIS documentation regarding persons and companies is indexed into the Defense Central Index of Investigations (DCII). Title change procedures ensure the proper identification on NCIS file information for both current and future retrieval. When an ROI (CHANGE) is submitted, it must reference the ROI (OPEN), ROI (ROPEN), or the last ROI (CHANGE) for the investigation. The reference listing must include the former master title and CCN, if either is different. Whenever an ROI (CHANGE) is submitted, it should specify exactly what information is being changed or corrected. If there are any offices that have outstanding/pending leads they must also be included in the top electrical destination, in the ACTION section and mailed a copy of the ROI (CHANGE), if the office does not have the capability to receive documents electronically.

c. Security Clearance. Place Code 024A under the INFO distribution section of the ROI (CHANGE) if there is a change in the subject and/or co-subject's security clearance. In the NCIS Report Writing, the "ELECTRICAL DISTRIBUTION" code for Code 024A (DONCAF) is /24A/.

25.1-5.6. ROI (INTERIM)

a. Used by the control office when reporting investigative findings/developments. The ROI (INTERIM) is used for external agency reporting purposes. For an example of an ROI (INTERIM), please refer to Sample (11). The ROI (INTERIM) will be prepared when:

(1) Reporting the status of the investigation consistent with the required reporting periods; or,

(2) Permanent change of case agent assignment is made after substantive investigative or operational effort was expended; or,

(3) The case is transferred from one NCIS office to another; or,

(4) All investigative action is complete but judicial, civil, or administrative action is pending. This ROI (INTERIM) will contain under the caption “ACTION”, the following statement to the responsible NCISHQ Department: "Active investigation completed. Case pending judicial/administrative action." The command or prosecutor may task the control office to conduct additional investigative tasks in refining the case for trial and a subsequent ROI (INTERIM) should report that task coverage. Non-NCIS control cases (i.e., specific phase type investigations) may be closed upon supervisory review if the case has been in an inactive status (i.e., pending judicial, civil or administrative action) for an extended period of time. Whenever a case is closed that is pending adjudication, an ROI (SUPP) is required to report final judicial, civil or administrative action.

b. All previous associated ROI (INTERIM) reports will be listed in the reference section.

c. Exhibits should be attached to the ROI (INTERIM), but in rare occasions there may be times when it is not prudent or feasible to attach exhibits. An example of this would be a joint investigation, when the lead agency is preparing a single all-inclusive report. In those rare occasions when command is not provided with exhibits or briefed, it must be noted in the ROI.

d. Transfer of Case Control. When primary investigative responsibility shifts between NCIS components, an ROI (INTERIM) with a “/T” disposition code after the CCN is required to effect the transfer. For the receiving office, the CCN will remain the same to include “/T”. Under the ACTION caption, an “R” is used to direct the transfer to the receiving component. Under the NARRATIVE caption, the text of the ROI will set forth the reason for transferring case control and describe any outstanding leads that are pending at other NCIS components or at the component transferring the investigation. If there are outstanding leads at other NCIS components, the ROI (INTERIM) should be transmitted electronically with an “R” action set forth under the ACTION caption directing all components with outstanding leads to report the results of those leads to the component assuming case control. Within ten (10) business days of receipt, the receiving component will acknowledge assumption of case control by an electronically transmitted ROI (INTERIM) to all affected components. It is the responsibility of the transferring component to ensure the transfer is completed. The CCN on all subsequent SSDs will continue to indicate the /T disposition code until the ROI (CLOSED) is transmitted. The ROI (CLOSED) and any subsequent documents (SUPP) will reflect the appropriate disposition code. Once transfer of control has been accomplished, to include transfer of case notes, there is no requirement for the former control office to routinely receive copies of documentation. The following are examples of relevant entries for an ROI (INTERIM) to transfer the case control from FEAJ to EUNA, and the subsequent assumption of control:

CONTROL: 28MAY08-FEAJ-0123-7NNA/T

ACTION
R. EUNA: Case control transferred to EUNA.
R. DIST: Provide results of outstanding tasks to EUNA.

ACTION
DIST: Case control assumed by EUNA.

25.1-5.7. ROI (CLOSED)

a. Submitted by the control agent after all investigative activity of the case is completed and all judicial, civil and/or administrative, or no action is reported for each subject, or co-subject in the NI Title. All associated ROI (INTERIM) reports will be listed in the REFERENCE section of the ROI (CLOSED). The ROI (CLOSED) should be a report that contains complete, accurate, and relevant information. The ROI (CLOSED) is intended for external agency reporting purposes. For an example of an ROI (CLOSED), please refer to Sample (12).

b. It is NCIS policy that resolved investigations will not be closed until disposition has been reported on all Subjects and Co-subjects of all NCIS controlled and joint investigations.

c. The ROI (CLOSED) can be utilized when an investigation was completed so timely as to preclude obtaining any benefit from the normal ROI (OPEN). The ROI (CLOSED) ONLY report will contain under the caption "ACTION" the following statement to the responsible NCISHQ Code: "ONLY Report." This caption is necessary to assist the professional support staff with handling procedures. It is mandatory to mail ALL ROI (CLOSED) ONLY reports to the RMB with the appropriate RIMS cover sheet. Any Special Interest (SI), DSI (Director's Special Interest), or Death Investigations will be mailed to Code 23 vice the RMB.

EXAMPLE:

ACTION
0023: ONLY Report

Additionally, the ROI (CLOSED), will be used when:

(1) Local law enforcement investigations on Department of the Navy service members are obtained and reported via NCIS Report Writing.

(2) The service member is documented in the NI Title as a subject or co-subject of an ROI (CLOSED), where their arrest by another law enforcement agency is being reported, an ROI (SUPP) is required following the subsequent adjudication of the matter.

(3) A complaint or incident, which falls within NCIS jurisdiction, is received but does not result in an open investigation. When this occurs, an ROI (CLOSED) is prepared identifying the incident, the source of information and a statement explaining the NCIS decision to refer the investigation to another agency. If NCIS declined to investigate the incident without further referral, an explanation is also required.

d. Security Clearance. When submitting an ROI (CLOSED), place Code 024A under the INFO distribution section if the subject and/or co-subject has a security clearance. In the NCIS Report Writing, the "ELECTRICAL DISTRIBUTION" for Code 024A (DoNCAF) is /24A/.

25.1-5.8. ROI (SUPP)

a. Used by control and lead offices when reporting supplemental information. Supplemental information may be obtained without additional investigative effort. (SUPP) documentation on closed investigations should include the appropriate disposition code with the CCN, and reference the last document submitted. The ROI (SUPP) is intended for external agency reporting purposes. When the ROI (SUPP) reports new information that changes or supplements information relevant to the collection of investigative data regarding a previously closed investigation, the case agent is responsible for updating the appropriate entries within the Consolidated Law Enforcement Operations Center (CLEOC) web application.

25.1-5.9. ROI (DISP) Special Requirement For CI/CT/Cyber Investigations

a. Required for all Category 3 and 5 investigations with an /F disposition code. Each subject and/or co-subject must have an individual ROI (DISP) at the conclusion of the investigation. Only one person or entity will be listed in the NI Title of the submitted ROI (DISP) for which the disposition information pertains. The text portion of the ROI (DISP) will have the data entries set out in columnar form under the caption heading "DISPOSITION". For an example of an ROI (DISP), please refer to Sample (13). Addendum (1) provides instructions for completion of the disposition worksheet. Addendum (2) is a disposition data worksheet and Addendum (3) provides a listing of attorney declination codes.

b. Under the DISTRIBUTION caption of each ROI (DISP), on the "ACTION" line, list the Subject of the investigation (e.g. S/NORTH, Jake Alvin/SGT USMC). This will permit cross-referencing of the titled person of the ROI (DISP) (co-subject or subject corporation) to the Master Title.

25.1-6. DATE ENTRY. All SSD documents will be dated in the same manner. The date will be entered day-month-year. The day will be a two-digit entry; the month, a three-letter abbreviation; and the year, a two-digit entry (e.g., March 19, 2008 would be entered 19MAR08).

25.1-7. CATEGORY ENTRY. On investigative or operational documentation, the Case Category entry will be the title set forth in Appendix (1) for the sub-category of the investigation being conducted (e.g., SABOTAGE for the sub-category 3F, GENERAL PROCUREMENT for the sub-category 4G, UNAUTHORIZED DISCLOSURE for sub-category 5D, DEATH for sub-category 7H, etc.)

25.1-8. PRIORITY LEVELS

25.1-8.1. All investigations will be prioritized at one of two levels when opened. Case prioritization is necessary to identify the level of investigative effort and timeliness reporting

requirements. Field components will assign priority levels; however, Priority (I) will not be assigned without prior consultation with the appropriate NCISHQ department.

25.1-8.2. Investigative Priority Levels

a. Priority (I) - Investigations and certain criminal initiative operations that have a major impact at the Seat of Government (SOG) level, involve national security or involve the operational capability or effectiveness of the Department of the Navy. Initial notification of a potential Priority (I) investigation will be made telephonically to NCISHQ via the NCIS Field Office as soon as possible following receipt of the information or complaint which generates the investigation. Some examples of Priority (I) investigations include:

(1) Joint NCIS/FBI espionage investigation.

(2) Investigation prompting major Executive Branch and/or congressional interest such as the attack against the USS Cole, and the terrorist attacks against the New York World Trade Center and the Pentagon.

(3) Other investigations of a highly sensitive nature where a high probability exists that NCIS has or will be tasked to respond to SOG inquiries.

b. Priority (II) - All other investigations, initiative operations, and ROI (INFO) reports will be designated Priority II.

25.1-8.3. The priority assigned to an investigation can be adjusted upward or downward during the investigation based on the merits of the case. When there is a change in the priority, the control office should submit an ROI (CHANGE) to notify the parent NCIS Field Office, NCISHQ and any lead components. Adjusting the priority of a case will be done after consultation with, or at the direction of, the appropriate NCISHQ department.

25.1-9. TIMELINESS REQUIREMENTS

25.1-9.1. Timeliness. All investigations should be completed and reported as expeditiously as possible. Timely reporting is linked to the priority level and type of report. It is impossible at the outset of an investigation to predict the actual time necessary to complete each case. It is a critical supervisory function to ensure timeliness in resolving issues, and substantiating and reporting findings. Expeditiously determining investigative strategy, reasonable expectations of completion, prompt publication of investigative reports, and reporting results of resolved investigations are mandatory supervisory responsibilities. Reporting requirements extend past the active investigative phase to include timely reporting of the disposition of subjects and co-subjects. Control offices may request expeditious handling of a lead in those circumstances where timeliness requirements are not sufficient to meet a critical need. Telephonic coordination should be made between the control field component and the lead field component before requesting expeditious handling. Upon receipt of tasking, the tasked NCIS employee should contact the case agent within three (3) business days via phone, fax, email, etc., to confirm or clarify tasking.

a. ROI (INFO). Transmit within ten (10) business days, after receipt of information. All ROI (INFO) reports have a Priority (II) designation.

b. ROI (OPEN)

(1) Priority (I) - Transmit within one (1) business day after receipt of information, which predicates investigation.

(2) Priority (II) - Transmit within three (3) business days after receipt of information, which predicates investigation.

c. ROI (ROPEN)

(1) Priority (I) - Transmit within one (1) business day after receipt of information, which predicates reopening the investigation.

(2) Priority (II) - Transmit within three (3) business days after receipt of information, which predicates reopening the investigation.

d. ROI (ACTION)

(1) Priority (I) - The tasked component will transmit results within five (5) business days, or sooner, after receipt of the task.

(2) Priority (II) - The tasked component will transmit status/results of lead tasking within ten (10) business days, or sooner, after receipt of lead.

e. ROI (CHANGE). Transmit within five (5) business days from the time that the new, or correct, information was obtained.

f. ROI (INTERIM)

(1) Priority (I) - Transmit within five (5) business days regardless of case category, including the ROI (INTERIM) following the completion of the last substantive investigative effort when awaiting adjudicative action.

(2) Priority (II) - Transmit within thirty (30) calendar days for all designated DSI and SI cases and death investigations (7H) in which NCIS is the primary investigative agency, or the lead or support agency in a joint death investigation for all cases in which the manner of death is homicide, suicide, undetermined, and all child deaths. Status reporting is 60 calendar days for 7H cases in which the manner of death is accidental and for all adult natural deaths. NCIS-3, Chapter 30 provides further guidance regarding timeliness and reporting requirements for death investigations.

(3) Priority (II) - Transmit within sixty (60) calendar days on all other case categories.

(4) Priority (II) - Transmit the ROI (INTERIM) within ten (10) business days after the completion of the last substantive investigative effort when awaiting adjudicative action.

g. ROI (CLOSED)

(1) Priority (I) - Transmit within five (5) business days from the last adjudicative disposition.

(2) Priority (II) - Transmit within ten (10) business days from the last adjudicative disposition.

(3) Priority (II) - Transmit the ROI (CLOSED) that serves as the ONLY document reporting information on an incident within ten (10) business days from receipt of the information.

h. ROI (SUPP) - Transmit within five (5) business days from the time that the supplemental information was obtained.

i. ROI (DISP) for CI/CT/Cyber Investigations. Transmit within five (5) business days from the time that the information was obtained.

25.1-9.2. ROIs may be submitted at any time substantive investigative information is developed. For instance, it is not necessary to wait for the 30/60 day due date to publish a ROI (INTERIM).

25.1-9.3. Investigative Action (IA). Complete the IA within five (5) business days from the day of collecting the information or performing the investigative act. The IA will be electronically transmitted along with the appropriate ROI.

25.1-10. CASE CONTROL NUMBER (CCN)

25.1-10.1. The assignment of a unique Case Control Number (CCN), which is not duplicated by another NCIS office, establishes an investigative file, which becomes an official record. The following guidance applies to all case categories, except case category 9Y, STAAT Activities (see 25.1-10.3. for guidance).

25.1-10.2. The following depicts the component parts that comprise elements of a CCN:

a. b. c. d. e. f.
17AUG08-NWBR-0050-6NNA/(single letter disposition code)

a. Control Date. The date that the NCIS component receives the complaint, information, or request, or the date the operation was initiated. The control date is not to be confused with the date of the ROI (OPEN) document. It is entered in the format of two digits for the day (e.g., 02, 12, or 27), three-letter abbreviation for the month, and two-digits for the calendar year. Some examples of control dates are: 20JUN08 and 05SEP08.

b. Originating Office. The four-character code of the NCIS component or NCIS department which either initiates the investigation or operation, or reports the opportunity collection of

information. The unique code for every NCIS element is set forth in the NCIS Office Directory (NCIS-2). Not all NCISHQ elements have issued NCIS-2 Data Sheets. Some Office Codes may need to be used at the HQ Division level, use the last four characters. The following are some possible examples of valid Originating Office CCN codes:

0024 (Operational Support Directorate)
024A (DoN Central Adjudication Facility)
024B (Field Services Support Department)
24B1 (Technical Services Division)
24B2 (Polygraph Services Division)
24B3 (Laboratory Services Division)
24B4 (Field Office Support Division (FOST))
24B5 (TSCM Support Division)
024C (Contingency Response Field Office (CRFO))
024D (Cyber Support Department)
24D1 (Cyber Investigations and Operations Division)
24D2 (Cyber Analysis Division)
24D3 (Cyber Technical Division)
24D4 (Atlantic Cyber Division)
24D5 (Pacific Cyber Division)
024E (Navy Information and Personnel Security Programs)
0025 (Intelligence Directorate)
025A (Operations Support Department)
25A1 (Operations/Investigations Support Division/RTP)
25A2 (Counter Terrorism Division)
25A3 (Cyber Support Division)
25A4 (Criminal Intelligence Division)
25A5 (Protective Service Support Division)
025B (Strategic Analysis Department)
25B1 (Americas and Pacific Division)
25B2 (Europe Division)
25B3 (Middle East Division)
025C (Warning and Production Department)
25C1 (Indications and Warning/Multiple Threat Alert Center)
25C2 (Production Division)

c. Sequence Number. Consists of four digits, beginning with 0001 and ending with 9999. Each NCIS component will maintain a CCN logbook that will record the assignment of sequence numbers. The same series of numbers will be used for assignment of CCN for investigation, operation, and opportunity collection. The sequence will be restarted at 0001 the beginning of every calendar year or at any time more than 9999 numbers are used during a calendar year in that office. The standard entries for the CCN logbook are: Case Agent; CCN Date; CCN Sequence Number; and CCN Project Code and title. After a calendar year has expired, that year's CCN logbook must be retained for an additional 2 years before destruction. For example, a CCN logbook ending 31 December 2007 would be retained all of 2008 and 2009 and destroyed in January 2010.

d. Case Category. Consists of two characters. The first character is numeric, representing the basic category of investigation. The second character is alphabetic, designating the sub-category within the basic category. CCN for Counterintelligence, Counterterrorism and Cyber operations have "XX" entered in the space for case category.

e. Project Code Identifier. Consists of two alphabetic characters that provide information for utilization in analysis of NCIS workload and identification of NCIS effort in certain program areas. There are separate groups of project codes that apply to investigations, operations and opportunity collection respectively. Project identifiers for case categories 4, 6, 7, and 8 are now captured through the CLEOC data screens under NCIS Investigative Responsibility, thus narrowing current code usage to those listed below in numbers 1 and 2. Project identifiers for CI/CT and Cyber investigations are listed in Addendum (4). Project identifiers for CI/CT and Cyber Operations and Information Reports [ROI (INFO)] are listed under numbers 3 and 4 below.

(1) Investigation Project Codes:

NA - Standard Navy Investigation
MA - Standard Marine Corps Investigation

(2) Criminal Operations Project Codes:

SO - Special Operation
UO - Undercover Operation

(3) Counterintelligence, Counterterrorism and Cyber Operations Codes:

CI - Counterintelligence Source Operation
CE - Offensive Counterintelligence Operation (replaces XXDA)
CT - Counterterrorism Collection Operation
IP - Infrastructure Protection
EX - Force Protection Exercise Support
FP - Force Protection
TP - CISPS (Technology Protection Support Packages)
RD - Support to Research and Development Facilities
TA - Support to Arms Control Treaties

(4) The following project codes apply to CCNs reporting opportunity/collection of information via the ROI (INFO):

CI - Opportunity collection of Counterintelligence information
CT - Opportunity collection of Counterterrorism information
CR - Opportunity collection of Criminal intelligence information
DS - Opportunity collection of Domestic Security information

f. Disposition Codes:

(1) General Crimes Investigations - For all criminal investigations, (Code 23), the only authorized disposition code for an investigation or operation is "/C."

(2) CI/CT/Cyber Investigations - The following disposition codes are authorized when closing counterintelligence, counterterrorism, and cyber crime investigations in case categories 3 and 5. No other disposition codes are authorized. The only authorized disposition code for an operation is “C”.

/C - to be used on all closed cases involving investigative, liaison and/or analytical effort to resolve non-criminal matters which were known at the initiation of the investigation. Examples would include the completion of a Force Protection (5C), Threat Assessment (5G), OPSEC Support (5M), and Personal Vulnerability Assessments (5V), Category 1 inquiries, and briefings (9F/9A).

/E - to be used in investigations where all leads were completed, but culpability could not be established (unresolved).

/F - used in closed investigations in which it was established that a crime did occur, suspect(s) identified, and culpability established (resolved).

NOTE: CI/CT/Cyber investigations closed with an /F disposition code require submission of an ROI (DISP) document. See Section 25.1-5.9.b. for guidance in preparation of a ROI (DISP) and needed codes.

/P - is used when the investigation determines the allegation of a crime is unfounded and the complainant knowingly made a false allegation.

/U - investigation determines no crime occurred (unfounded).

(3) Do not use a disposition code for ROI (INFO) reports.

25.1-10.3. CCNs for STAAT Activities. The following guidance applies to CCNs with the standard system document for recording STAAT activities. The following example depicts the component parts that comprise elements of a CCN:

a. **b.** **c.** **d.** **e.** **f.**
01APR08-0021-8001-9Y02/C.

a. Control Date. "01APR08" is the Control Date, the date the operation was initiated. It is entered in the format of two digits for the day (e.g., 01, 12, or 27), three-letter abbreviation for the month and two-digits for the calendar year.

b. Originating Office. "0021" is the Originating Office, which remains constant (HQ Code 21).

c. Sequence Number. "8001" is the Sequence Number based on a block of numbers assigned to your unit per below. Sequentially record activities. Do not skip any numbers. In the example, "8001" is the first report of the calendar year for Singapore. The second report would be "8002", etc. Each STAAT unit will maintain a CCN log that will record the assignment of sequence numbers. The sequence will be restarted with the first number in the assigned block (e.g., 8001) at the beginning of every calendar year or at any time all numbers in your block have been exhausted during a calendar year. Assignments for each office are as follows:

0001 to 0999 - NCIS Headquarters
1001 to 1999 - NCISFO Norfolk
2001 to 2999 - NCISFO Southeast
3001 to 3999 - NCISFO Europe
4001 to 4999 - NCISRA Sigonella
5001 to 5999 - NCISFO Southwest
6001 to 6999 - NCISFO Northwest
7001 to 7999 - NCISFO Far East
8001 to 8999 - NCISFO Singapore
9001 to 9999 - NCISFO Bahrain

d. Case Category. "9Y" is the Case Category and remains constant. "9Y" identifies the report as a STAAT product.

e. Project Code Identifier. Specifies the type of work (or project) that was done, as listed below:

9Y01 - CNOIVA
9Y02 - PIVA
9Y03 - MSC SHIP IVA
9Y04 - ASSISTANCE VISIT
9Y05 - TRAINING
9Y06 - IG SUPPORT
9Y07 - AT/LE EXERCISE
9Y08 - SECURITY POST VALIDATION
9Y09 - MWD ASSIST/VALIDATION
9Y10 - FP READINESS REVIEW
9Y11 - ASSESSMENTS, OTHER
9Y12 - STAAT, OTHER

f. Disposition Code. "/C" is the Disposition Code, which indicates the project is "closed," meaning there is no further input expected to this report.

25.1-11. CASE TITLE

25.1-11.1. Except for Report Writing SSD General Administration (Gen Admin), which is prepared in memorandum format, all SSDs are prepared in a format that uses master and secondary titles. These titles are the means by which NCIS investigations are indexed and cross-indexed into the DCII and in NCIS Central Files. There are two (2) general types of master and

secondary titles: Personal Titles (Subject, Co-subject, Victim, Alias/AKA and Nee); and Impersonal Titles (Generic/Incident). Each specific type of title is indexed into a file by a name identifier (NI) code. Every investigation, operation, etc. will have a master title and can have any number of secondary titles. At a minimum, the master and secondary titles for subjects, co-subjects, and victims will reflect social security number and/or date of birth and/or place of birth (presumptive for a foreign national, when appropriate, such as in a category 3D (Contact Report) investigation). Absent this data, no person will be listed as the master or secondary title. Correct and accurate title information is essential for retrieval of file information and identifying records. Guidance for changing master title entries from generic/incident titles to Subject or Victim titles, and for correction or adding to title information is set forth in Section 25.1-5.5 (Person Title Entries). In joint investigations, there must be a consistency among the investigative agencies in titling the investigation. The identities of the persons and companies titled, the full names of those titled, and spelling of those names will be identical in each agency's reporting.

25.1-11.2. Deletion of a titled subject, co-subject or victim of an investigation will be done only with the approval of the Director, NCIS (see NCIS-1, Chapter 23 for additional guidance). Therefore, the titling of a person or non-person in the subject title must be properly evaluated based upon the guidelines in 25.1-11.3.a. and b.

a. Identifying information about the subject of a criminal investigation shall be removed from the title block of an ROI and the DCII in the case of mistaken identity; i.e., the wrong person's name was placed in the ROI as a subject or entered into the DCII.

b. Identifying information about the subject of a criminal investigation shall be removed from the title block of an ROI and the DCII if it is later determined a mistake was made at the time the titling and/or indexing occurred in that credible information indicating that the subject committed a crime did not exist.

25.1-11.3. Name Identifier (NI) Title. The master title of the investigation or operation is referred to as the NI Title. The NI Title is comprised of the following components:

a. **b**. or **c**. **d**.
S/JOHNSON, THOMAS MATTHEW/HM3 USN
M/W/NEE3/S/123-45-6789/28JUN72/MESA, AZ
e. **f**. **g**. **h**. **i**. **j**. **k**.

NOTE: Supplemental information and/or duty station may be added below the NI Title entries.

a. Role Identifier Code. The following is a listing of the NI codes that describes the role of the person or non-person entered into the title:

(1) S/(SUBJECT)

(a) In all criminal investigations, a person, company and/or organization is titled as a subject if there is credible evidence that a crime was committed and more than mere suspicion exists that the person, company, and/or organization was the principal in the crime.

Determination whether there is credible evidence is based upon: (1) do you have allegations that if found to be true would constitute an offense, (2) do you have allegations by someone who has a basis for knowledge, and (3) are there indications of reliability of the person making the allegation. This equates to some substantiation or corroboratory evidence beyond the initial allegation. For example, an anonymous hotline complaint should not be the sole basis for titling a person as a subject. The anonymous complaint may be the basis for the initiation of a generic titled investigation. Until there is some substantiation of the individual's involvement, a person, even if named by the anonymous complainant, should not be put in the title block. If the complainant makes a sworn statement concerning the individual's direct involvement in a crime, this is ordinarily the basis for placing the individual in the title block. In those cases, the identifying data of a person is to be entered as a NI title vice opening or maintaining an investigation under a generic/incident title. The standard for making the determination on whether a person is entered into the NI title should not differentiate between the type of the offense being investigated. A person may be placed in the title block based on information from another law enforcement agency if, in accordance with their policy, they have made the individual a target of their inquiry. All person(s) listed in the S/ or X/ block MUST be interviewed. If a person requests an exculpatory polygraph based upon allegations not investigated by NCIS, the person will be entered as a subject regardless of the merits of the information or command investigation. Normally the person suspected of the most serious offense(s) will be the listed subject if more than one suspect is implicated. If a military member and a civilian are both suspected of the offense(s), the military member is the listed subject. A subject title may only be listed as a master title. In the text, S/(TRUE LAST NAME) will be used when referring to the subject of the investigation. For example, "S/NORTH admitted the theft" vice "Subject admitted the theft."

(b) In all CI/CT/Cyber investigations, categories 3 and 5, the "credible information threshold" theory cannot be clearly applied. In a CI investigation or in matters of national security, a prosecution may not be the result or even the goal of the inquiry. CI/CT/Cyber cases are often initiated simply upon the receipt of a credible allegation. The significance of the information that is obtained during a CI/CT/Cyber investigation may not be apparent at the time of its receipt; therefore, it is imperative such information can be retrieved. It is recognized that investigative data captured and closed under a generic titled inquiry is not retrievable, therefore, the value of the individual involvement will be lost, and the impact to national security could potentially be placed in jeopardy. When deciding whether to title an individual or entity, the investigating agent will coordinate with the SAC, ASAC, or SSA who will use their respective professional judgments concerning the titling of subjects/co-subjects of CI/CT/Cyber investigations.

(2) X/(CO-SUBJECT)

(a) In all investigations, a co-subject is any person, company, or organization other than the subject, who is suspected of participating in the offense or acting in concert with the subject of the investigation. The same criteria used to title a subject will be used to enter a co-subject as a secondary title. When preparing a narrative report, X/(TRUE LAST NAME) will be used when referring to a co-subject of the investigation in the text. For example, "X/SOUTH admitted he bribed the official" or "X/ SMITH admitted he lost the classified document." For individuals with the same last name, when preparing a report, use the last name accompanied by the full first

name. For example, “X/SMITH, Michael admitted that he assisted X/SMITH, Thomas in procuring the illicit drug paraphernalia.”

(3) V/(VICTIM): Victim is a person, company, organization or government activity against which a crime is committed. .

(4) A/(ALIAS OR "ALSO KNOWN AS" [AKA]): Used to list other names used by a person, company, or organization. Alias or aka is always a secondary title.

(5) N/(NEE): Used to identify a married woman by her birth name (maiden). NEE is always a secondary title.

(6) I/(GENERIC/INCIDENT): Used when a suspect or victim is not known. Example: I/WASHINGTON DC/INCREASED USE OF ECTASY.

b. Person Title Entries

(1) A person's name will be entered after the Role Identifier Code in the following manner: surname, followed by a comma and a space; first given name or initial followed by space; and middle name(s) or initial(s). Names should always be used in preference to initials. Addendum (5) provides guidance for the name coding procedure for surnames that are not the typical singular surname. If a Roman numeral, such as II or III, is used, or a suffix, such as Jr., or Sr., is used, place it directly after the surname. Such suffixes should be considered as part of the surname. There should be one space between the surname and the suffix. Do not use any punctuation to separate the surname and the suffix. The following is an example for John Henry Barley-Corn Jr.:

S/BARLEYCORN JR, JOHN HENRY/CIV

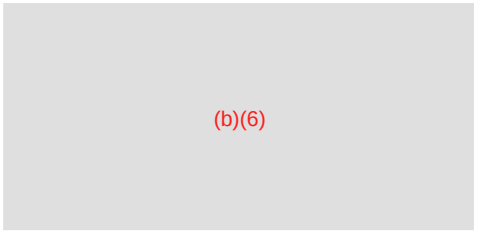
(2) In the case of married women, the married surname should be used. The birth name should be entered as a (N/) title. Additional guidance for name entries, including surnames with prefixes, compound names, and foreign names, is contained in Addendum (5) to this chapter.

(3) Because of the importance of this issue, the following is restated for emphasis. The master and secondary titles for subjects, co-subjects, and victims will reflect social security number and/or date of birth and/or place of birth (presumptive for foreign national when appropriate, such as in a category 3D (Contact Report) investigation). Absent this data, no person will be listed as the master or secondary title. Examples are as follows:

(a) The below master title with V/SMITH.

(b)(6)

(b) The below UNDESIRABLE examples occasionally occur when reciprocal assistance is provided to local police departments. In such cases, attempts should be made to obtain one of the identifiers set forth. If not obtained, a generic title should be utilized.



(c) In summary, every effort should be made to obtain full identifying data on persons listed as Subject, Co-Subject, and/or Victim in the investigation. Full identifying data, including security clearance information, on all DoD personnel is mandatory prior to case closing. Efforts to obtain such data on civilians (from police, motor vehicle or employment records, etc.) must also be made.

(d) A single exception to the above guidance occurs when the investigation involves unidentified human remains. The identity may be unknown for some time. To facilitate retrieval of the case file, indexing of the unidentified remains will be accomplished by titling the remains as a victim with the pseudonym of DOE, JOHN, DOE, JANE or DOE, UNKNOWN. If the sex cannot be determined, the remains should be entered as indeterminate. If an anthropologist gives an opinion as to the probable sex, it should be entered as that sex. Titling protocols to be used in death investigations with unidentified human remains are as follows:

V/DOE, JOHN (NMN)/UNK
M/U/ZZZZ/N///

V/DOE, JANE (NMN)/UNK
F/U/ZZZZ/N///

V/DOE, UNKNOWN (NMN)/UNK
Z/U/ZZZZ/N///

(e) If multiple remains are found together, entries should be made using the protocol of including in the middle initial position A, B, C, etc., to signify the total number of remains titled. Examples of multiple titling are:

V/DOE, JOHN A/UNK
M/U/ZZZZ/N////

V/DOE, JOHN B/UNK
Z/U/ZZZZ/N///

c. Non-Person Title Entries.

(1) Generic/Incident Titles. This master title is used when credible evidence does not exist to title a suspect, or when a suspect has not been identified and there is no known victim. Incident titles will be listed in the following order:

Name (facility-unit-activity), Location (city, state or city, country), of the incident or situation involved.

EXAMPLE:

I/SAN DIEGO, CA /DESIGNER DRUGS BEING SOLD IN DOWNTOWN
BUSINESS DISTRICT

(2) Non-Person (Subject/Victim). This master title is used when a company or organization is listed as the SUBJECT or VICTIM.

(b)(6)

V/NAVAL AIR STATION
CORPUS CHRISTI, TX

(3) Non-Person (Project Indicator). Used in sensitive investigations and operations as a means of protecting the identity of the subject or subject matter under investigation. A project indicator will only be assigned by the responsible NCISHQ Department and will be centrally controlled by NCISHQ. Once a project indicator has been assigned, it will be used on all subsequent SSD documentation, including that forwarded by mail. The closing document should reflect the subject title under which it was opened.

d. Person - Status Entries.

(1) A person's title status entry is a narrative description of an individual's rank or grade within the U.S. Government. For a non-U.S. Government employee and most retired military members, a descriptive term as to that individual's status is appropriate and in most cases will simply be "CIV" to describe the person's civilian status. The title status entry appears after the name. An example would be: (b)(6) MAJ USMC. The following pertains to personal title status entries for U.S. Government military and civilian personnel:

(a) For military personnel, the entry will reflect current rank/rate, branch of service and status, (e.g.: LT USNR; BM1 USN; MAJ USMC, LCDR JAGC USN).

(b) For Civil Service personnel, the entry will reflect the individual's status, (e.g., GS, GM, GG, WG, ES, NSPS pay schedules, etc.), and grade/pay band, (e.g., GS11, ES01, YM02).

(c) For non-government personnel, the narrative status description would be "CIV".

e. Person - Gender Codes. The SSD system provides pick-lists that include three choices for gender. They are:

M : Male
F : Female
Z : Unknown

f. Person - Race Codes. The SSD system provides pick-lists that list the currently accepted race codes.

I : American Indian/Alaskan Native
A : Asian/Pacific Islander
B : Black
W : White
U : Unknown

g. Person - Status Identifier Codes. A data field used to code a person's status. The field is divided into two groups of two characters each. The first two characters are alphabetical and define the general military, civilian, or other status of the individual. The second two characters may be alphabetical, numerical or a combination of both. The code provides the person's status, rank or grade. See Addendum (6) for the use of the two groups of characters. For government employees who are under a pay system not reflected in Addendum (6), use equivalent GS grades.

h. Person - Security Clearance Code. A security clearance code MUST be entered for this field, and the SSD system provides a pick-list menu with the authorized entries. This entry is for the level of security clearance currently held by the individual or that no security clearance is held. DoD affiliated persons who are subjects or co-subjects of an investigation must have an entry other than "U" for unknown in this field. For purposes of this entry, the term DoD affiliated persons includes active duty and reserve military personnel, civilian personnel of the DoD and the Military Departments and employees of DoD contractors or their subcontractors. The Security Clearance Code "N" will be used only when there is an actual determination that the person has not been granted a security clearance. It is always preferable that the security clearance level be obtained when the subject/co-subject is/are first titled in the NI Title. Place Code 024A on distribution of the ROI (OPEN), ROI (ROPEN), ROI (CLOSED), or ROI (CHANGE), when there is a change in the subject and/or co-subject's security clearance. The NCIS Report Writing "ELECTRICAL DISTRIBUTION" for 024A (DoNCAF) is /24A/.

i. Social Security Number (SSN). The SSN should be listed in numerical format. Leave blank if SSN is not known or if individual has not obtained one.

j. Date of Birth (DOB). Enter the person's date of birth in the format of two-digit entry for day, three-letter abbreviation for month, and two-digit entry for year with no spaces for the digits and letters. Example: 05NOV64.

k. Place of Birth (POB). Enter the geographic location of the person's birthplace by listing city (if known) and state if the person was born in the United States. For persons born in the U.S., the state entry should be the postal abbreviation, see United States Post Office link at http://www.usps.com/ncsc/lookups/usps_abbreviations.html. However, if the person was born outside of the United States, then enter the city (if known) and country of the individual's

birthplace. Ensure to spell out the country name, since the use of the two-letter country abbreviation could result in duplication of abbreviations for U.S. states. The current DCII listing of country names and codes is found on the Infoweb under the Administrative Services Department website, “Tools” page.

NOTE: Place of Birth entries are character-size limited. If over the size limit, place in supplemental section or text of initial ROI report.

l. Supplemental Data (SUPP)/Duty Station (DUSTA). Supplemental Data provides amplifying data as to the identity or status of the person or company/corporation being indexed. When personal title entries are made for military personnel and an individual's duty station is different from the military command listed in the Command section of the SSD, a DUSTA entry is mandatory (e.g., DUSTA: NAS OCEANA, VA). If an individual is the Commanding Officer, Executive Officer, Security Officer, Personnel Officer, or other staff/management position, that status should show as SUPPLEMENTAL DATA. When information is developed that a subject or co-subject is an inactive Navy or Marine reservist, the reserve affiliation with rank and branch of service will be entered here. If the individual is retired military, that information should also be entered here. The following are examples of personal titles with Supplemental Data:

(b)(6)

S/ANYNAME COMPANY
WASHINGTON, DC
SUPP: 1123 NE 17TH STREET

25.1-12. COMMAND LINE

The command entry normally consists of the caption “COMMAND” followed by a slash (/); the Standard Navy Distribution List abbreviation for the activity or command primarily affected by the investigation, followed by a slash (/) and the five-digit Unit Identification Code (UIC) or Reporting Unit Code (RUC) for the activity or command. In instances where there is no command, use the phrase “DOD interest” or “NON-DOD interest”, with “UIC 00000”.

EXAMPLE: COMMAND/NAVSTA NORFOLK VA/60188
COMMAND/NON-DOD INTEREST/00000

An ROI (CHANGE) must be submitted if there are any changes to the command line and/or UIC/RUC.

25.1-13. MADE AT LINE. The MADE AT LINE consists of the specific office code, location, and name of the reporting person.

25.1-14. REFERENCES

25.1-14.1. Sample (14) is an example of an ROI with a field for REFERENCES. If not used, the reference field should be deleted from the template. Any reference will be listed under the caption by alphabetic character in parentheses, beginning with (A) and continuing through the alphabet, including double letters if required. For example, (Z) would be followed by (AA), (BB), etc. No document should be listed both as a reference and exhibit on the same SSD document. References will be listed in the order they are discussed in the text of the SSD and all references listed must be mentioned in the text. However, it is not necessary to discuss ROI (INTERIM) reports, which are listed solely for the purpose of identifying prior ROI (INTERIM) reports generated throughout the course of the investigation/operation. All previous ROI (INTERIM) reports pertaining to the specific case will be listed in chronological order in the reference section of each subsequent ROI (INTERIM) report and on the final ROI (CLOSED) report. This will occur even if no exhibits were attached to the referenced ROI (INTERIM) report. Doing so allows the reader a quick view of the generated reports and associated exhibits. Additionally, it ensures they are aware of all case reports, including classified ROI (INTERIM) reports, which are needed for administrative action and/or trial preparation.

25.1-14.2. Do not reference telephone conversations. The conversation, unless recorded, cannot be reconstructed and not all recipients have access to the conversation. However, if significant or pertinent information is developed during a telephone conversation, then the details should be memorialized in an Investigative Action (IA) and appended as an Exhibit to a ROI. References will be typed in upper and lowercase letters consistent with the Navy Correspondence Manual, except for naval messages that are required to be typed in UPPER case.

a. ROIs (with the exception of those documenting undercover or special operations and Cooperating Witness records) are documents which are subject to release outside of NCISHQ. Therefore, documents primarily used for internal agency purposes (e.g., ROI (ACTION)s, Gen Admins, NCISHQ Manuals and directives, ROI (INFO)s reporting SO, UO or CW matters) will not be listed as references on ROI (CLOSED), (INTERIM) or (INFO) reports.

25.1-14.3. A classified document can be listed as a reference on a SSD without classifying the SSD. However, if the title of the referenced document is classified, then the listing of it makes the SSD a classified document.

25.1-14.4. When an NCIS SSD or case is listed as a reference, follow the below examples for format:

REFERENCES
(A) NCISRU USS Carl Vinson ROI (ACTION)/26Jun08
(B) NCISRA Pascagoula MS ROI (CLOSED)/03Sep08/S/DOE, John Lee/
CCN: 01SEP07-GCPA-0356-3XNA
(C) NCISFO Hawaii-Pearl Harbor HI CASE FILE: I/Vigilant Pacific 2008 (U)/
CCN: 02AUG08-HIHN-0255-XXEX

25.1-14.5. If the title of the reference is a document, directive, manual, etc., then the word "Subj" with a slash (/) and the title is required.

REFERENCE
(A) OPNAVINST 5510.1H/Subj/DEPARTMENT OF THE NAVY INFORMATION AND PERSONNEL SECURITY PROGRAM REGULATION

NOTE: The NCIS Manuals or General Administrations (Gen Admins) should never be referenced on any ROI.

25.1-15. EXHIBITS

25.1-15.1. Any document or other item attached for transmittal with an SSD will be marked and listed as an exhibit on the SSD. DO NOT USE an SSD as a means of transmittal for any items maintained in the NCIS Evidence Custody System. The listing will be under the caption "EXHIBITS." See Sample (15), Sample (16), and Sample (17) for templates showing placement. If there are no exhibits, the caption should be deleted. Exhibits, less Investigative Action documents, will be forwarded on an ROI (INTERIM) when requested by NCISHQ or the customer during the investigation. Exhibits will also be forwarded on an ROI (INTERIM) for cases designated SI or DSI. Otherwise, exhibits will not be sent to NCISHQ during the investigation but will be noted under the REFERENCES caption when referencing previous ROIs. This will be done by listing the relevant ROI, followed by the caption "Contains Exhibit #" or "Contains Exhibits # - #" in parentheses. This caption will be used even if only one exhibit is listed.

The NCIS Manuals or Gen Admins should never be made an exhibit to any ROI.

EXAMPLE:

REFERENCE
(A) NCISRA Quantico VA ROI (INTERIM)/07May08 (Contains Exhibits 1-15)

25.1-15.2. List the exhibit by number in parentheses and in the order in which the exhibit is listed in the text of the SSD. Exhibits will be sequentially numbered throughout the investigation regardless of the number of ROI (INTERIM) reports prepared. To illustrate this point, if four (4) ROI (INTERIM) reports are written and each ROI has two (2) exhibits, the first ROI will reflect exhibits (1) and (2); the second ROI will reflect exhibits numbered (3) and (4), and so on. When listing the exhibit, a description of the exhibit will be included. This description will include the date of the document, for example, IA: Results of Interview of V/JONES, JOHN/25Apr07. The text of the IA will document the date the reported activity was conducted. If the exhibit depicts a scene on a particular date, such as in a photograph or crime scene sketch, the description should include the depiction date of the scene. If the date is unknown, the document should be described as "undated." Each listed exhibit will show the distribution of the exhibit. When the transmittal of any original document is involved, the recipient of the original document should be clearly indicated. The following are exhibit listings using upper and lowercase letters:

EXHIBITS
(1) Map depicting location of Pier 9/undated. . .(Copy All/Less 0024A)
(2) IA: Crime Scene Examination/10Aug08. . .(Copy All)

(3) Statement by (b)(6) 11Aug08. . .(Original 23B/Copy All)
(4) IA: Results of Interview of SUBJECT/15Aug08. . .(Copy All)

25.1-15.3. If the exhibit is in an electronic media format (e.g., CD, DVD, etc.) the title of the electronic file (i.e., exhibit) contained in the media will follow the same fundamental naming convention prescribed for non-electronic exhibits, except it will include the word "EXHIBIT" in the name. This is particularly critical if the exhibit is sent to NCISHQ for insertion. Properly labeling the exhibit in the electronic media will better ensure that it is properly identified and inserted into the proper place in the electronic closed case file. This will also aid in the proper identification and retrieval when retrieving the file in RIMS. The following is an example of the proper way to title the file in the electronic media:

EXHIBIT (1) Video of crime scene/25Aug08

25.1-16. ENCLOSURES

25.1-16.1. A document attached to an EXHIBIT is called an "ENCLOSURE." Attached enclosures should be listed on the relevant exhibit under the caption "ENCLOSURES" (or if only one enclosure is listed, the caption "ENCLOSURE" should be used instead). Enclosures should be marked and described in the same manner as exhibits. However, distribution information should not be included in the enclosure's description. When marking the enclosure, use alpha characters in UPPER CASE only. For instance, if Exhibit (12) has three enclosures, they would be listed on the exhibit as (A), (B), and (C). This caption will be used even if only one enclosure is listed, as in the example below:

ENCLOSURE
(A) Waiver of Rights Form S/SMITH/10Apr08

25.1-16.2. If the enclosure is in an electronic media format (e.g., CD, DVD, etc.) the title of the electronic file (i.e., enclosure) contained in the media will follow the same fundamental naming convention prescribed for non-electronic enclosures, except it will include the words "ENCLOSURE ( ) to EXHIBIT ( )" in the name, with the associated enclosure and exhibit identifiers included. This is particularly critical if the enclosure is sent to NCISHQ for insertion. Properly labeling the enclosure in the electronic media will better ensure that it is properly identified and inserted into the proper place in the electronic closed case file. This will also aid in the proper identification and retrieval when retrieving the file in RIMS. The following is an example of the proper way to title the file in the electronic media:

ENCLOSURE (A) to EXHIBIT (1) Video of crime scene/25Aug08

25.1-17. ATTACHMENTS

25.1-17.1. A document attached to an ENCLOSURE is called an ATTACHMENT. Attachments should be listed on the relevant enclosure under the caption "ATTACHMENTS." The caption should be used whether attaching one or more to the associated enclosures. The attachments should be labeled with an alpha character in lower case. As an example, if

Enclosure (A) has three attachments, the attachments would be labeled (a), (b) and (c). An example:

ATTACHMENT
(a) Signature Card provided by V/DAVIS/23May08

25.1-17.2. If the attachment is in an electronic media format (e.g., CD, DVD, etc.) the title of the electronic file (i.e., attachment) contained in the media will follow the same fundamental naming convention prescribed for non-electronic attachments, except it will include the words "ATTACHMENT ( ) to ENCLOSURE ( ) to EXHIBIT ( )" in the name, with the associated attachment, enclosure and exhibit identifiers included. This is particularly critical if the attachment is sent to NCISHQ for insertion. Properly labeling the attachment in the electronic media will better ensure that it is properly identified and inserted into the proper place in the electronic closed case file. This will also aid in the proper identification and retrieval when retrieving the file in RIMS. The following is an example of the proper way to title the file in the electronic media:

ATTACHMENT (a) to ENCLOSURE (A) to EXHIBIT (1) Video of crime scene/25Aug08

25.1-18. MARKING OF EXHIBITS, ENCLOSURES, AND ATTACHMENTS

25.1-18.1. All exhibits, enclosures, and attachments must be marked for identification. This marking will be at the lower right hand corner of the first page of the document, and will consist of the word "EXHIBIT" or "ENCLOSURE" or "ATTACHMENT" followed by the number or letter for that document in parentheses, e.g., "EXHIBIT (1)" or "ENCLOSURE (A)" or "ATTACHMENT (a)". When original documents, such as statements, are attached as exhibits or enclosures, they shall not be altered in any manner. Typing in or stamping an exhibit number or enclosure letter on the original document is considered an alteration. For those original documents, a small slip of paper with the exhibit or enclosure number typed or stamped on it should be affixed to the lower right hand corner of the first page of the document.

25.1-18.2. Exhibit Numbering. The following protocols will be utilized to ensure the integrity of sequentially numbering exhibits, enclosures, and attachments to ROI (INTERIM) and (CLOSED) reports, and to maintain control and accountability of the marking process.

a. Exhibit numbers will be continuous throughout the investigation. For example, the first ROI (INTERIM) might contain Exhibits (1) through (13). The second ROI (INTERIM) would then start with Exhibit (14), and so on.

b. If the exhibit was previously numbered and attached to a ROI (INTERIM) report, then that same number should be used when referring to the exhibit in any subsequent ROI (INTERIM) reports. Since each exhibit number is unique, it is not necessary to state in the NARRATIVE portion which ROI (INTERIM) the exhibit was attached to because its location will be easily discernible.

c. Tasked offices responding to a lead by ROI (ACTION) will number the exhibit(s) beginning with exhibit one (1). When the control agent reports out the lead tasking in the next control office ROI (INTERIM), any exhibits received from tasked offices will be assigned the next sequential exhibit number of the control case.

d. If an investigation is closed and an ROI (SUPP) is subsequently submitted, the exhibit numbers on the SUPP should begin where the ROI (CLOSED) numbers left off. For instance, if the ROI (CLOSED) contained exhibits (18) and (19) then the ROI (SUPP) should begin with Exhibit (20). In the event an investigation is reopened, the above policy also applies.

25.1-19. CRIMINAL FINGERPRINT CARDS AND MUG SHOT PHOTOGRAPHS. The following procedures will be utilized when submitting criminal fingerprint cards and mug shot photographs to NCISHQ Code 24B3. Guidance for completing the fingerprint card (FD-249) is contained in OPNAVINST 5530.14D, paragraph 1209. Additionally, guidance for criminal history reporting requirements is contained in NCIS-3, Chapter 6 (Investigative Theory and Procedures).

a. Certified Mail. Two (2) criminal fingerprint cards (FD-249), and associated mug shot photographs, will be submitted to NCISHQ for processing and filing with the FBI and shall be sent with an ROI (ACTION) via certified mail to:

NAVAL CRIMINAL INVESTIGATIVE
SERVICE HEADQUARTERS
ATTN CODE 24B3 FINGERPRINTS
716 SICARD ST SE SUITE 2000
WASHINGTON NAVY YARD DC 20388-5380

b. In the ROI (ACTION), NCIS Code 24B3 should be listed in the ACTION line, with no response required to this tasking (see example below). Additionally, the certified mail number for the submitted fingerprint cards and mug shot photographs should be stated in the ACTION line. The certified mail number will be maintained by the submitting unit or field office to track submissions. Fingerprint cards and mug shot photographs are not to be shown as exhibits.

EXAMPLE:

ACTION
24B3: Submission of criminal fingerprint cards (2) and mug shot photographs (2) are for inclusion into the FBI database. Tracking number: 0000000000.

c. Biometrics Units. If previously mailed to NCISHQ, do not submit fingerprint cards electronically via biometrics units (Livescan) as this results in the creation of a duplicate criminal history record.

NOTE: NCIS-3, Section 30-17.3., Original Victim Fingerprint Cards, provides additional guidance regarding the handling of original fingerprint cards for victims.

d. Mug shot photographs. Mug shot photographs that are mailed with the two original criminal fingerprint cards will be scanned by Code 24B3 and included with the electronic fingerprint record that is sent to the FBI/CJIS. Once the criminal history record is accepted by the FBI/CJIS, Code 24B3 will prepare the mug shot photographs for file retention. The requirements outlined below must be followed when preparing mug shot photographs for submission to NCISHQ Code 24B3.

(1) One mug shot photograph must be a full facial frontal, and the second and third mug shot photographs must be 90 degree right and left profiles.

(2) Mug shot photographs must be a standard 4" x 6" print, preferably in color.

(3) Do not submit photographs via electronic or digital storage media (i.e., e-mail, CD, or DVD) as these cannot be processed; however, 4" by 6" prints from digital cameras or other electronic means are acceptable for submission.

(4) The following information should be entered either below or affixed to the back of the mug shot photograph:

(a) Case title;

(b) Subject/co-subject's name;

(c) Subject/co-subject's social security number; and

(d) Case Control Number.

e. These requirements apply only to mug shot photographs enclosed with the original fingerprint card submission and not to the submission of other case file photographs.

25.1-19.1. Case File Photographs. Photographs may be submitted via electronic media (e.g., CDs, digital media sticks, etc.), but will continue to be accepted in paper form. The following procedures will be used when submitting case file photographs in paper form.

a. To facilitate imaging, the stacking of photographs on a single sheet fan-style, or over-lapping, and placing the documentation for each photograph on reverse/back side is prohibited. Ongoing electronic scanning processes require that all information be contained/visible on the front side of a standard 8 ½” x 11” sheet of paper. Thus, 8” x 10” size photographs must be attached with clear tape to a sheet of paper with identifying data, either above or below the photograph. Two or more smaller size photographs, where/when acceptable, may be placed on a single sheet with identifying data, but may not overlap. The minimum identifying data provided on the sheet is the Case Title and the Case Control Number (CCN), photograph number, and the enclosure or exhibit number. See NCIS-3, Chapter 30 (Death Investigations) for additional information. Photographs or pictures that contain child porn will not be placed in the case file per Title 18 USC 2252.

(1) The attached photograph will be at least 4"x 4" in size and attached to an 8 ½" x 11" piece of paper. The following information should be below the photograph: case title; subject/co-subject's name, rate & service designation (if different from case title); subject/co-subject's social security number; CCN; and Case Agent/Office.

(2) If the attached photograph is a Polaroid, affix the subject/co-subject's name and social security number on the back of the picture, as well.

25.1-20. EXECUTIVE SUMMARY. One line below this caption begins paragraph one (1). The Executive Summary (ES) text provides a concise investigative summary that conveys major findings in the investigation to-date. The ES portion is limited to one paragraph. The ES portion is used by NCISHQ for briefing purposes. Therefore, the ES paragraph header is only required on ROI (INTERIM) and ROI (CLOSED) reports. Information contained in all other ROI reports can be captured under the NARRATIVE paragraph header. Additionally, when the ROI (CLOSED) is submitted as an "ONLY Report," the ES section is unnecessary, and all information can be contained in the NARRATIVE portion.

25.1-21. NARRATIVE TEXT PROTOCOLS FOR SSD

25.1-21.1. The NARRATIVE is utilized as the second caption following EXECUTIVE SUMMARY when both are utilized as captions in the ROI (INTERIM) and ROI (CLOSED). The first line below this caption begins with paragraph one (1) and is followed by subsequent numbered paragraphs. NARRATIVE paragraphs should provide the customer with an understanding of the major facts of the investigation developed during the reporting period. The caption NARRATIVE is used in all ROIs regardless of status.

a. The first sentence of the first paragraph of the NARRATIVE portion should clearly state the reason for case initiation; (i.e. reactive, reciprocal, details and disposition, etc.) and if applicable, contain the relevant statute(s) that is/are suspected to have been violated.

b. Exceptions to this requirement are:

(1) Criminal investigation under the case category "DEATH." "No determination of a specific statute can be made at this time."

(2) For CI and CT investigations the following statement should be used: "This investigation is being conducted as a (counterintelligence matter) or (counterterrorism matter)."

25.1-21.2. SSD Text

a. The portion of the SSD text, excluding the "header" or "footer," is referred to as the "body." Narrative text is typed in upper and lowercase letters and begins after any or all listings of REFERENCE(S), EXHIBIT(S), and/or CAVEATS. Unlike the ROI, there are no captions in the body of a Gen Admin. See Sample (18) to view an example of an SSD ROI. Captions not used will be deleted for that document.

NOTE: When referring to individuals within the body of the text, the last name is typed in all UPPER-CASE LETTERS (i.e., (b)(6) The first and middle name will be typed in upper-lower case letters when used the first time. Use the last name for subsequent references to the individual.

b. The use of distasteful words or phrases in the body of the report is inappropriate. The exact words a perpetrator used in obscene telephone calls, extortion and other similar cases must be reported; however, the appropriate location for such words is in a victim's statement or results of interview. It is sufficient to report in the text of the ROI that the perpetrator solicited sodomy or oral copulation vice using the street vernacular.

c. The use of agent's notes is not authorized on SSD documents.

25.1-21.2. Gen Admin. The body of the Gen Admin consists of numbered paragraphs. Alpha characters in parentheses and numbers in parentheses will be used for subparagraphs. See Sample (19).

25.1-21.3. ROI and IA. Will consist of numbered paragraphs, which report or direct investigative or operational actions. Arabic numerals with a period, Alpha characters with a period, Arabic numerals in parentheses, and alphabetic characters in parentheses, in that order of utilization, will be used for subparagraphs, per the following example:

1.

a.

(1)

(a)

See SECNAVINST 5216.5D, Figure 2.7. Standard Letter Paragraph Formats, for further guidance.

25.1-22. LISTING OF PARTICIPANTS. The identification of all investigative personnel participating in an investigative or collection action will be reported under the caption "PARTICIPANTS" in the ROI. The caption and the listing will appear after the final paragraph of the narrative and before any action. In addition to NCIS personnel, the listing may include other investigative personnel who participated in the NCIS investigation. The reporting agent's name will not appear under the caption. In addition to listing names, the title and organization for each individual should be included. The following are examples of PARTICIPANTS entries using upper and lowercase letters. An exception to this guidance is entries on naval messages where format requires all capital letters. Provide name, title, agency and location.

PARTICIPANTS
(b)(6) Special Agent, NCISRA Great Lakes, IL

(b)(6)	Agent, MPI, PMO, MCB Camp Pendleton, CA etective, NYC Police Department

25.1-23. ACTION: USE OF INVESTIGATIVE AND ADMINISTRATIVE TASKING

25.1-23.1. Direction for NCIS components and NCISHQ to perform investigative or certain administrative actions are set forth under the caption “ACTION.” The specific directions for the type of investigative or administrative actions to be taken are set forth under the caption by denoting the NCIS four (4) character component office code followed by a colon (:) then two spaces and the description of the action to be taken. If more than one office component is tasked for the same action, multiple four-character component codes can be entered on the same line separated by a slash (/). The four-character component code may be replaced by the entry "DIST," which means the action is for all addressees.

25.1-23.2. Guidance pertaining to the use of the “R” Code

a. The “R” code requires a response. The following are examples of conditions when the “R” code is appropriate for use.

(1) The indicated component has investigative or operational activity set forth for coverage,

(2) Control of the investigative case has been transferred to the indicated component and/or,

(3) The indicated component is being directed to discontinue previously received tasking(s) and report investigative activity to date, to include action not taken.

b. The “R” code will not be used if:

(1) The report is sent for corrections to the case title/CCN.

(2) The tasking is used to advise the responsible NCISHQ Department “Active investigation completed. Case pending judicial/administrative action.”

(3) The tasking is used to forward criminal fingerprint cards to NCISHQ Code 24B3.

(4) The indicated component is being directed to cancel previously received tasking(s) and a response is not required due to the cancellation of the original tasking.

25.1-23.3. Upon receipt of lead tasking, the tasked office will respond utilizing an:

a. ROI (INFO) report - if the tasking was sent via an ROI (OPEN) or ROI (INFO); or

b. ROI (ACTION) report - if the tasking was received via any other ROI report type. Another ROI (ACTION) will be used subsequent to the submission of the completed ROI (ACTION), and reference the previous ROI Action.

25.1-23.4. The last paragraph of the ROI report, used to report completion of lead tasking, will include the following statement: “Lead tasking is complete.”

25.1-23.5. The following are examples of ACTION entries:

ACTION
R.EUNA: Obtain handwriting exemplars from (b)(6)
R.EURT: Apprise USS NEVERSINK of this investigation.
R.DCWA: Locate and interview Capt (b)(6) USMC, regarding his knowledge of (b)(6) association with (b)(6)
R.NEPH/NELH/NEPP: Query local law enforcement in your area to determine if (b)(6) was a suspect in thefts of electronics.
FOXX: Provide copies of this Gen Admin with exhibit (1) to components within your Field Office.
22B1: Provided for action deemed appropriate.
R.NWEV: Tasking requested via Reference (A) is cancelled. Report investigative activity to date.

25.1-24. CORRECTIVE ACTION PROCESS

a. The Corrective Action Process for ROIs and IAs was developed as a result of a need for an agreement between the legal issues governing records management and legal issues pertaining to the integrity of NCIS investigative files for court presentation or Freedom of Information Act release. This section sets forth information regarding the proper method to correct transmitted SSDs that contain errors in the header and/or the text. The relevant SSDs are Report of Investigation (ROI) and Investigative Action (IA).

(1) "Administrative/Typographical" errors will be addressed by transmitting a revision of the ROI or IA. The ROI will contain an ACTION section to DIST explaining in detail the information that was erroneously reported and detailing the revisions that have been made to the ROI. The IA will include a paragraph before the first numbered paragraph in the body of the IA explaining in detail the information that was erroneously reported and detailing the revision(s) that has been made to the IA. Please note the revised ROI must be provided to all of the parties it was originally disseminated to including any external commands/parties that were provided with a hard copy. The following is an example of an ACTION section in a ROI:

ACTION
DIST: Please note the original transmission of this ROI inaccurately reflected the status code as (INFO) vice (CLOSED). This transmission accurately reflects the status code as (CLOSED) and supercedes all others. Any previous transmissions of this ROI should be destroyed and replaced with this ROI.
0023: Please delete any previous transmissions of this ROI from this CCN in the NCISHQ Case Information System.

Samples (20) through (23) are examples of the transmission of ROIs containing administrative/ typographical errors and examples of revisions of the ROIs with the ACTION section detailing the errors that have been corrected.

The following is an example of the paragraph to insert when transmitting a revised IA:

“Please note the original transmission of this IA inaccurately contained duplicate numbering of paragraphs as 3. and reflected the sequence number in the Case Control Number (CCN) as 0123. This transmission accurately numbers the paragraphs and reflects the accurate sequence number in the CCN as 0124. Any previous transmission of this IA should be destroyed and replaced with this IA.”

Sample (24) is an example of the transmission of an IA containing an administrative/ typographical error. Sample (25) is an example of the revised IA with the added paragraph, which is inserted prior to the first numbered paragraph, providing the specifics of the error being revised.

(2) Text Errors: "Text" information for ROI documents is defined as information contained in the Narrative and Executive Summary sections. The "Text" portion of IA documents is defined as the actual body of the report, which documents the investigative action taken and being reported.

(a) The text provides the investigative details and therefore, the text of the document should never be changed, unless the error is strictly an administrative or typographical error. Any corrections/revisions to the investigative details that have been reported must be outlined in a subsequent INTERIM report. “Administrative and typographical errors” describes (for instance) writing “there” when “their” or “they’re” was intended, or assigning two (2) enclosures the same alphabetic character listing in the Enclosure Section of the IA.

(b) Text ROI: NCIS field components detecting any non-administrative/typographical error(s) in the text of a ROI will ensure the error(s) is/are outlined in the next ROI (INTERIM) or (CLOSED) report, as applicable. The incorrect ROI will be referenced, a detailed explanation of the error(s) will be provided, and the ROI will detail the accurate information that was intended to be reported. The ACTION section of the ROI will be to DIST and state the ROI details and provides clarification regarding the error(s) outlined in the inaccurate referenced ROI.

(c) Text IA: NCIS field components detecting any error(s) in the text of an IA will ensure the error(s) is outlined in the next ROI. The relevant IA will be referenced and the ROI will provide as an exhibit a follow-on IA addressing the error(s). The revised IA will include the following sentence as the first paragraph of the text:

This revised IA only addresses the error(s) contained in the referenced incorrect IA identified in the accompanying ROI. This revised IA does not report any new or additional investigative information in relation to the investigative action being reported.

(3) Oftentimes administrative and/or typographical errors are not discovered until numerous ROI and/or IA documents have been transmitted. To avoid creating an extra work load, when administrative and/or typographical errors are detected and the documents are no longer held in the Word SSD system for modification it will be sufficient to transmit an ROI (CHANGE) directing pen and ink correction to the pertinent document(s). However, please note if the error

is contained in a document that impacts the storage of information in the NCISHQ Case Information System (CIS) or the NCISHQ Case Management System (CMS), the document will need to be recreated and retransmitted. ROI (OPEN), (ROPEN), (CLOSED), and (INFO) documents impact the storage of information in the NCISHQ CIS for Code 0023 investigations. An ROI (CHANGE) document can impact the storage of information in the NCISHQ CIS, depending on the information being changed. If each NCIS Field Office ensures all CIS Error Messages are addressed in a timely manner and if every office ensures all ROIs are transmitted this will eliminate the need to re-type any documents because they will still be stored and can be retransmitted to the appropriate NCISHQ Department.

(4) If the error(s) are not detected until after a case is CLOSED, the vehicle to report and detail the correct information will be an ROI (SUPP). This guidance also pertains if the ROI generated is a CLOSED Only Report or an INFO. However, if the error resulted in the rejection of the ROI (CLOSED), including Only Report, or the ROI (INFO) from the CIS, a CIS Error Message will be received at the pertinent Field Office, which will detail the error. Please refer to the section on CIS Error Messages.

(5) Revised ROIs and IAs should only be transmitted to correct certain typographical and administrative errors. The guidance concerning the submission of ROI (CHANGE) documents outlined in Section 25.1-5.5. a. and b. of this chapter details when it is appropriate to submit a ROI (CHANGE) to modify existing information. For further clarification, ROI (CHANGE) documents will be submitted to add individuals or non-person entries to the title block, to add or modify additional or existing identifying data, to modify other title block information for an existing individual or non-person entry, and to modify the command or made at lines. "Corrected Copy" will never be typed on any ROI/IA documents.

b. CIS Error Messages: Each ROI and IA transmitted to Code 23 undergoes error checking by the CIS application. The CIS reads and checks the documents starting with the Case Category entry up to and including the Made At Line. Upon detecting an error, the CIS generates an error message, which will be forwarded to the appropriate NCIS Field Office or NCISHQ Department. Each NCIS Field Office and pertinent NCISHQ Departments are responsible for designating a point of contact who will receive these error messages via the point of contact's individual email account. In the event the point of contact is not available for an extended period of time (a week or more), it is the responsibility of the field office or pertinent headquarters department point of contact to notify, via email, the NCISHQ coordinators to identify an alternate point of contact.

(1) Pertinent Case Categories: Only case categories 2A, 2M, 2S, all 4, all 6, all 7, all 8, 9A and 9P investigations are affected by the CIS Error Messages. The CIS Error Message for the pertinent ROI/IA will print out at the field office identified by its two-character code in the "Made At" line. For headquarters, it is the four-character code identified in the "Made At" line.

(2) How the process works: Any ROI/IA with error(s) will be saved to a Microsoft email and sent from NCISHQ CIS to the person serving as the point of contact (POC) designated by each field office and headquarters department. The email "Subject" line is "ROI/IA Errors in (and identified the date, time and Operating System Queue [OSQ] of the document)". Below the "Subject" line, the email text identifies that an error was detected and directs a review and

modification of the ROI/IA. Below the email text, separated by a line, is a copy of the actual ROI/IA. At the end of the ROI/IA is another separation line. Below this line is an explanation of the error and on what line, when applicable, of the ROI/IA the error(s) is/are found. The POC will ensure the revision and retransmission is accomplished. For the field office, the POC will be responsible for further disseminating the error message to the subordinate office that generated the ROI/IA.

EXAMPLE OF CIS ERROR MESSAGE WARNING:

ERROR WARNING: This incident is not in the CIS Data Base.

ERROR INDICATES: This error indicates the CIS cannot find a CCN that matches the CCN on the transmitted ROI or IA.

ERROR MESSAGE GENERATED AS A RESULT OF:

1. The Control Date, Originating Office or Sequence Number in the CCN contains a typographical error, is invalid and/or not recognized.

2. The ROI (CLOSED) Only Report or the ROI (INFO) was not transmitted prior to transmitting IAs for the CCN. This will result in the receipt of a CIS Error Message with this Warning because the ROI (CLOSED) Only Report or the ROI (INFO) must be transmitted first to create the case in the CIS.

3. If the office has not transmitted the OPEN to 0023 the CIS will not be able to store the subsequent ROI and/or IAs. The OPEN must be transmitted first to create the case in the CIS.

(a) It is not possible to cover the necessary corrective action for every possible nuance pertaining to typographical and administrative errors. Therefore, any questions should be directed to the NCISHQ Code having responsibility over the pertinent investigative case category. Points of contact are as follows:

Code 21 (Counterterrorism Dept.)
Case Categories: 5C, 5T, 5Y, XXCT, XXFP and XXEX.

Code 21B (Protective Operations Dept.)
Case Categories: 5V and 9A.

Code 22 (Counterintelligence Dept.)
Case Categories: 1L, 1X, 3C, 3D, 3F, 3G, 3X, 5A, 5B, 5D, 5E, 5F, 5M, 5X, 9F, 9V, XXCI, XXCE, XXTP, XXRD and XXTA.

Code 23 (Criminal Investigations Dept.)
Case Categories: All 4, 6, 7, 8 and 9P.

Code 24D (Cyber Dept.)
Case Categories: 5I, 5H, 5J, 5K and XXIP.

25.1-25. DISTRIBUTION/DISSEMINATION OF CASE DOCUMENTATION

25.1-25.1. “DISTRIBUTION” Caption

a. The caption "DISTRIBUTION" is the last administrative entry that appears at the end of the body of the SSD. Entries set forth under this caption identify NCIS components, military commands and/or other agencies that are being provided copies of the SSD and the method of distribution.

b. Under the DISTRIBUTION caption, left margin justified, are potentially three types of sub-captions that are used; NCISHQ, ACTION and INFO followed by a colon (:). The entries following those sub-captions will be the four character NCIS component code, commands and agencies names where distribution external to NCIS is being made. The distribution code for NCISHQ should only reflect the code with responsibility for the investigation/operation. Multiple entries are separated by slashes. Authorized codes for the methods of distribution, in parentheses are: (M) for mail; (F) for facsimile; (H) for hand-carry; (P) for Procomm, (SIPR) for SIPRNET email, and (E) for email dissemination.

25.1-25.2. Dissemination of NCIS SSD Reports

a. Internal Dissemination of NCIS SSD.

(1) When using the report writing system, the transmission line for reports will begin with //, followed by the last two alphabetic letters of the field office code (or three or four digit HQ code), followed by //. If more than one office is listed, the offices will be separated by a slash.

EX: //21/PF/24C/IZ/22B1/MP/NA/WA//

(2) Due to changing needs by NCISHQ and its customers regarding what specific documents are needed during the pendency of an investigation designated Priority I or “DSI” or “SI”, NCISHQ Codes will notify the affected component and designate what documentation is needed.

(a) For further information to maintain documentation during the pendency of the case, such as the standard case file setup, standard case management forms, etc., in preparation for submission to NCISHQ, see NCIS-1, Chapter 45.

(b) Detailed information regarding the special reporting requirements for Death Investigation (7H) cases is contained within NCIS-3, Chapter 30. Timeliness requirements apply as set forth in Section 25.1-9.

(3) The DON Central Adjudication Facility, NCIS (Code 024A) will receive an information copy of the ROI (OPEN), ROI (CHANGE), and the ROI (CLOSED), when the subject or co-subject(s) has a security clearance. Code 24A is mandated to review the security clearances of all individuals identified in cases of criminal misconduct.

(4) The NCISHQ Special Intelligence Communications (SPINTCOMM) 24x7 Watch, NCIS Report Writing Electrical Destination - /NN/ (NCIS Code 0015N3) will continue to serve as the 24x7 centralized point-of-entry for all NCIS National Crime Information Center 2000 (NCIC-2000) database record-Entry transactions. The NCISHQ SPINTCOM - 00NN will receive an Action copy of any ROI when NCIC-2000 Entry documentation is required.

(5) NCISHQ Records Management Branch (RMB) is the central records center for all case documentation and ultimately must receive "original" photos and/or “best” copies of all documentation (i.e., ROI, exhibit, enclosure, attachment) generated as the result of the investigation. It is the responsibility of the control field component to ensure that NCISHQ is provided that documentation at the conclusion of the investigation. The following guidelines are to be followed in closed cases. It is mandatory to mail ALL ROI (INFO) and ROI (CLOSED) ONLY REPORTS to the RMB with the appropriate RIMS cover sheet. Any Special Interest (SI), DSI (Director’s Special Interest), or Death Investigations will be mailed to Code 23 vice the RMB. No evidence will be sent to RMB. Evidence will be stored in the appropriate field component’s evidence facilities.

(a) Where material is not sent electronically, the field will package closed investigative case files sent to NCISHQ using the following Finished Files (Records Management Division) standards:

1. Copy any fax material that is on thermal paper or microfilm information to bond paper before sending.

2. Remove all duplicate copies.

3. Separate all perforated pages; remove perforated printer guide tracks and place pages facing the same direction.

4. All documents will be in date order, starting with the open at the bottom and ending with the closing at the top.

5. Each document will be two-hole punched at the top/center and attached with two-hole paper fasteners. If the material is small enough a single staple in the upper left hand corner is acceptable.

6. Ensure all staples (an exception is made for staple cited in subparagraph (5), above), paper clips, binder clips, and rubber bands are removed.

7. Avoid sending light or illegible copies. Make every effort to obtain a good quality document. If a bad quality document is the best available; ensure this is indicated on that document by using a "BEST COPY AVAILABLE" stamp.

8. When highlighting case documentation, use a yellow highlighter. Any other type of highlighter will black out the highlighted area when copying.

9. Ensure that the case is complete with all case documents and exhibits. If missing unclassified documents are unavailable, a Memorandum for the Record (Missing Material from Dossier), dated and signed by the field supervisor, is required identifying the missing material. A copy of the Memorandum for the Record (Missing Material from Dossier) is also found on the Administrative Services Department intranet website on the Tools page. Guidance for utilizing and completing the Memorandum for the Record is contained in the Guide for DCII and Case File Preparation, which is currently being updated by Code 11C1, Records Management Branch. For further guidance, contact (b)(6) Head of Records Management or (b)(6) Assistant Head of Records Management at the following e-mail addresses: (b)(6)

10. Electronic media (i.e., computer disks, CDs, DVD, digital media sticks) may be included in the case file. When the electronic media is included, it must be clear where the media belongs in the case file. If an exhibit, enclosure or attachment, insert a page labeled with the exhibit, enclosures or attachment identifiers and a brief description of the contents of the media. This will be accomplished by using the guidance for completing the Cross-Reference Sheet and itemizing the items that are being sent separately. This guidance (DCII Guide and Case File Preparation) and the Cross Reference Sheet are contained on Administration's intranet website on the NCISnet.

NOTE: All electronic media submitted to NCISHQ is subject to FOIA review and disclosure. To alleviate the time consuming review of extraneous material and streamline the FOIA disclosure process, agents submitting electronic media (i.e., CDs containing digital photographs, the contents of downloaded computer hard drives etc) must limit the material being submitted to only that which is materially relevant to the case. Extraneous material should be maintained in the locally held case file. Only the relevant material (which has been listed as an enclosure or attachment to an IA or ROI) should reside on the electronic media forwarded to NCISHQ for permanent retention. Video and audio recordings (in CD or DVD format) may be included in the case file forwarded to Headquarters. As a reminder, electronic media containing child porn must not be placed in the case file per Title 18 USC 2252.

11. For two-sided documents, photocopy the reverse. Using a yellow highlighter or a pencil, lightly draw an "X" on the reverse of the original page and place the pages in proper consecutive page order in the file.

12. Legal (8 ½" x 14") size documents must be reduced to letter 8 ½" x 11" size.

13. Attach a "Records Information Management System Coversheet," signed and dated by the Supervisory Special Agent (SSA), for each case forwarded to NCISHQ.

(b) These standards are in place to ensure a high quality product when the investigative material is inserted into the imaged closed case file. The Cross-Reference Sheet must be properly filled out with the case number and other pertinent information or it may be impossible to marry the material to the proper electronic closed case or to easily locate the proper place to insert the material in the closed case file.

(c) The Finished Files Checklist can be used to ensure quality control is completed at the local office. It will not be included in the case file package. The Finished File Checklist is located on Administration's intranet website on the NCISnet. Utilizing the same standards, all DSI/SI investigations and operations should be mailed to the appropriate operational code at NCISHQ. Additional guidance pertaining to DSI/SI can be found in section 25.1-28.

b. External Dissemination of NCIS SSD

(1) The official description of the NCIS Investigative Files System, set forth in NCIS-1, Chapter 21 lists all routine uses for records from the system, as well as identifying those categories of users who are exclusively authorized to receive them. The "routine uses" should be taken specifically from System Notice N05520-4, NCIS Investigative Files System (June 30, 1998, 63 FR 35578).

(2) No NCIS field component is authorized to directly provide NCIS reports or files to members of Congress, congressional committees or the General Accounting Office. All such requests must be forwarded to NCISHQ (Code 000L) for action and appropriate response.

(3) For external dissemination, the document must be attached to a Document Cover Sheet (DCS) (NCIS Form 5000). Normally, dissemination of a SSD is made to an authorized user for use and disposal as appropriate. However, the sensitivity of the information included in the SSD may require more restrictive handling of the document. Additionally, the DCS may forward information furnished by another agency that is controlled by special handling caveat. In these cases, paragraph two (2) of the DCS should be annotated. Final disposition of the document should also be annotated in paragraph three of the DCS and will be signed by a NCIS special agent manager or acting supervisor (i.e., SAC, ASAC, SSA, or Acting SSA).

(4) Dissemination of SSDs to addresses external to the Department of Defense requires compliance with the disclosure accounting procedures of the Privacy Act of 1978, if a subject, co-subject or victim is indexed as a master or secondary title. Disclosure accounting procedures, including the use of a paragraph in the SSD with the caption of DISCLOSURE ACCOUNTING, is set forth in NCIS-1, Chapter 21. When appropriate, the listing of DISCLOSURE ACCOUNTING will be the last paragraph of the Narrative.

c. Acquisition, Use, Retention, Further Dissemination of Non-DoD Agency Records.

(1) Any non-DoD agency (i.e. local police department) records acquired as part of an official NCIS investigation can be made part of the NCIS investigative file in the following manners:

(a) The special agent may review the local agency records and summarize them in an NCIS Investigative Action; or,

(b) The local field office may have a preexisting agreement with the local agency that the local agency's records can be maintained and disseminated by NCIS as if the records belonged to NCIS; or,

(c) In all other cases, local agency records must be obtained with the use of the request to Obtain Non-DoD Records form NCIS form 5580/97. The form should be printed and taken with the NCIS representative, when the acquisition of a local police department record is anticipated. All information must be filled in and both the providing agency official and the NCIS representative receiving the non-DoD agency record must sign and date the form. The completed form will be labeled as an "Enclosure" to the Investigative Action (IA) with the non-DoD Agency record appended as an "Attachment" to the "enclosure" section. See sections 25.1-16, ENCLOSURES and 25.1-17. ATTACHMENTS.

25.1-26. INVESTIGATIVE DATA SUBMISSIONS

25.1-26.1. It is imperative that investigative data be input at the beginning, during, and before the investigation/inquiry is closed. Case data regarding NCIS investigations and the adjudicative outcomes are required and will be entered into the Consolidated Law Enforcement Operations Center (CLEOC) web application, if the case is reported via SSD instead of DONCJIS. The data supports the NCIS analysis program; input to semiannual reporting required under the Inspector General Act of 1978; and, to meet other reporting requirements levied by Department of Defense and Department of the Navy.

25.1-26.2. If reported via SSD, all case category 4, 6, 7, and 8 investigations require the entry of data into CLEOC. ROI (INFO), SO and UO operations are excluded from this requirement. For all others, any level of investigative effort (preliminary or formal), in which the incident is documented under a CCN, applicable data will be entered. For one time reporting of an incident, in which there is a one-time reporting, (e.g., ROI (CLOSED) done within 10 business days), data will be entered at a minimum under, “Incident,” “Offense Status,” and “Subject/Victim” screens through CLEOC.

25.1-26.3. NCIS offices will submit the details of case adjudication (charges, findings/verdicts, sentences, administrative or civil sanctions) in the text of the closing ROI and ensure all documents supporting the actions are included as exhibits.

25.1-26.4. If there is to be a press release regarding an NCIS investigation/operation, all criminal, civil and administrative documentation must be forwarded to NCISHQ (via FAX) on a real time basis. It is the responsibility of the control agent and field supervisor to ensure thorough on-line review, adherence, and accuracy of the collection and reporting of investigative data pertaining to the case, case titled individuals, and/or companies.

25.1-27. SSD REPORT CAVEATS. Investigative findings, which are collected and reported in SSDs or by naval message, may contain information that by law, policy or directive requires specific handling procedures. Notification of this requirement is made through the use of a caveat, which will appear on the SSD. Addendum (7) lists the only authorized caveats to be used and discusses placement of caveat.

25.1-28. DIRECTOR’S SPECIAL INTEREST “DSI” DESIGNATION. The designation “DSI” for Director’s Special Interest is NOT a priority categorization; it does denote this agency’s interest in an investigation requiring monitoring and potential briefs to senior level

managers/leaders. For the complete guidance on DSI and Special Interest (SI) cases, refer to NCIS-1, Chapter 45.

25.1-29. SPECIAL REQUIREMENTS IN GRAND JURY REPORTING

a. Grand Jury reporting will not occur during the pendency of an investigation, unless required by NCISHQ. All case updates ROI (INTERIM), transmitted electronically, should provide sufficient information to enable required briefings.

b. Grand Jury actions will be recorded via ROI (SUPP), following the submission of the ROI (CLOSED). The Grand Jury ROI (SUPP) and material subject to rule 6(e) will be sent via U.S. Registered Mail in the following manner:

(1) ROI (SUPP) will record ONLY the Grand Jury series of events.

(2) ROI (SUPP) will include the Grand Jury Caveat: "Grand Jury Material - Disseminate Only Pursuant To Rule 6, Federal Rules of Criminal Procedure", see Addendum (7).

(3) Include ONLY those Grand Jury documents that directly contribute to, and report the results of, prosecution(s). Examples: Grand Jury Evidence directly related to the outcome/prosecution(s), Grand Jury Subpoenas and Judgment Orders. No other Grand Jury documents should be forwarded to NCISHQ. Contact the cognizant NCISHQ Desk Officer if you have any questions regarding what to forward to NCISHQ. Grand Jury material will not be imaged. It will be retained in its existing format and will be submitted to RMB for storage. A Cross Reference Sheet must be completed and attached to the Grand Jury material when sent to RMB. Guidance for the Cross Reference Sheet preparation is contained in the DCII Guide and Case File Preparation located on Administration's intranet website on the NCISnet. The Cross Reference Sheet is also contained on Administration's intranet website or the Downloads section of the NCISnet.

(4) Forward the ROI (SUPP) with the attached Cross Reference Sheet to NCISHQ, double wrapped via registered mail:

(a) Inner envelope should display the following:

1. Grand Jury Caveat on front and back

2. NI Title

3. CCN

(5) Identify the contents, i.e., NENP ROI (SUPP) dated DDMMMYY.

(a) Outer envelope – USPS registered mail to NCISHQ.

(6) Coordinate with the local prosecuting attorney to determine what material is, or is not, Grand Jury and what may, or may not, be forwarded.

25.1-30. CYBER INVESTIGATION DATA SETS (CIDS). The Computer Investigations and Operations Division CIDS collects data for the NCIS Sentinel database for all case categories 5H, 5I, 5J, and 5K, to populate the JTF-CNO LE/CI Center database, and provide the field agent with an investigative guide. The theory is that if all required documents are obtained and all fields are completed, the investigation has been solved. The CIDS will be incorporated as the second paragraph on all aforementioned NCIS reports and will be used by the supervisors in conducting case review to ensure continual progress is being made in the investigation. Any entry that is unknown should be initially left blank; however, every attempt should be made to fill in all CIDS categories by the time the investigation is closed. However, if certain CIDS cannot be completed, leave it blank. Do not use "None" or "N/A". Fields requiring more than one data category can be duplicated as many times as possible. Addendum (8) contains data sets for seven of the fields, to include a list of country codes. Addendum (9) provides a breakdown of these fields in nine categories, as they should appear in the text of the report. Sample (26) is a sample ROI (OPEN) using the nine categories.

25.1-31. PRESENTATION SUMMARY

25.1-31.1. A presentation Summary (PS) will be prepared for the adjudicative authority, i.e., convening authority, trial counsel, US Attorney's office. If preparation of the PS is deemed non-essential by the adjudicative authority to develop trial strategy, or to the integrity of the historical dossier, the field supervisor may waive the preparation of this document. Sample (27) is an example of a PS.

25.1-31.2. Specific Guidance for a Presentation Summary

a. The PS is a single document that is "Appended" to the ROI (INTERIM) as a REFERENCE. This allows existing exhibits, enclosures, and attachments to be affixed to the PS as is, and eliminates the need to rename/renumber them.

b. Any case exhibits/enclosures/attachments attached to the PS will retain their previously assigned numbers. If the exhibits/enclosures/attachments were never assigned official numbers, then they should be assigned numbers when attached to the PS. However, unless the PS is the only case reporting mechanism, it should not contain exhibits/enclosures/attachments that were not previously reported via a ROI (INTERIM) report. Should there be an exhibit/enclosure/attachment not previously reported in a ROI, subsequent ROIs shall document them.

c. If an exhibit is not specifically discussed in the PS, then it is not necessary to list it on the PS. Relevant exhibits should be listed on the PS in numerical order, but may be referenced throughout the PS in any order necessary.

d. If enclosures and/or attachments are discussed in the body of the PS, they should be referred to by their assigned letter/number designation. Additionally, the associated exhibit should be listed on the PS. Because the exhibit is listed, it is not necessary to list the enclosures/attachments, as their association with the listed exhibit will be readily discernible.

e. The PS is the only report that may be attached to the ROI (INTERIM) being used to submit it. This ROI (INTERIM) may not be used to report new case details.

f. When a PS is attached to an ROI (INTERIM) report, the reference line will contain the words "Presentation Summary" followed by the date completed and the word "Appended" in parentheses. Example:

REFERENCES
(A) NCISFO Europe, Naples IT, ROI (INTERIM)/07May08 (Contains Exhibits 1-15)
(B) Presentation Summary/25Jun08 (Appended)

g. If a PS was previously provided, it will be listed in the REFERENCE(S) section of subsequent ROI (INTERIM) and ROI (CLOSED) reports, minus the word "Appended," but followed by the caption "Contains Presentation Summary" in parentheses. Example:

REFERENCES
(A) NCISFO Europe Naples IT ROI (INTERIM)/07May08 (Contains Exhibits 1-15)
(B) NCISFO Europe Naples IT ROI INTERIM)/25Jun08 (Contains Presentation Summary)
(C) NCISFO Europe Naples IT ROI (INTERIM)/18Aug08 (Contains Exhibit 16)

Pages 567 through 654 redacted for the following reasons:
- -
(b)(7)(E)

CHAPTER 26
TITLE: FACILITY MANAGEMENT AND ENGINEERING
POC: CODE 11A
DATE: JAN 08

26-1. GENERAL

26-1.1. Introduction

This chapter outlines the planning, programming, roles, and responsibilities established to assure the provision and management of NCIS facilities. It amplifies and augments information found in OPNAVINST 11010.20G, "Facilities Project Manual," NAVFACINST 11010.44E, "The Shore Facilities Planning Manual," and NAVFACINST 11010.45D, "Comprehensive Regional Planning Instruction," regarding NCIS mission requirements, workforce dynamics and the rapidly changing security and law enforcement environment. The final section of this chapter is a glossary of key facility terms.

26-1.2. Background

NCIS personnel operate from more than 150 locations worldwide. One or more facilities are occupied at each location. NCIS facilities fall predominantly into the administrative use category, but they include evidence warehouses, polygraph facilities, forensic laboratories, and the Multiple Threat Alert Center (MTAC) – an operations and intelligence nerve center located within the NCIS Headquarters (NCISHQ) building at the Washington Navy Yard. Most NCIS facilities are aboard Navy and Marine Corps bases and stations. The remainder are located in General Services Administration (GSA) owned/leased spaces, other service bases, allied bases, embassies, and aboard naval vessels. Additionally, NCIS has a presence at several Force Protection Detachments (FPD) located in embassies and consulates throughout the world. While the Department of State is responsible for meeting FPD facility requirements, NCIS has financial responsibility for space and services provided at FPDs for which NCIS is the executive agent. The many types and broad distribution of NCIS facilities presents a challenging facility management environment with respect to maintaining situational awareness and positive host-tenant relations. Continuous NCISHQ and Field Office (FO) engagement is required to ensure that current and future NCIS facility requirements are met.

26-1.3. Mission

The mission of the NCIS facility management and engineering organization is to, ensure that NCIS facilities are adequate in capacity, features, and condition; fulfill forecasted facility requirements in a timely manner that supports operations without delay or disruption; provide

each employee with a suitable workspace where and when it is needed; provide workspaces that contribute to employee productivity, satisfaction, and retention; and create the conditions that allow facility costs to be forecasted, programmed, controlled, and avoided.

26-1.4. Facility Management Defined

Facility management is the practice of coordinating an organization's physical workplaces with its people and work. Facility managers integrate people with purpose and place, harnessing the principles of engineering, architecture, finance, business administration, and the behavioral sciences to optimize the utility, quality, and economy of an organization's work environment.

26-2. THE NCIS FACILITY PLANNING CYCLE

26-2.1. Description

The Facility Planning Cycle is a systematic means by which the NCIS facility mission can be accomplished. The Facility Planning Cycle describes the continuous process of, determining future facility requirements, assessing existing facilities, comparing existing facilities to future requirements to identify facility deficiencies, developing facility projects (and/or other actions) to correct the deficiencies, obtaining resources to execute the facility projects, and executing the facility projects. Facility assessments are revised to reflect improvements, and the cycle begins anew. The NCIS Facility Planning Cycle operates within a challenging planning environment.

26-2.2. Environment

Operating within the Department of the Navy (DON), the NCIS facility planning environment features, challenging and evolving law enforcement and intelligence missions; intense resource competition; deliberate facility project and budget processes; rigid facility regulations augmented by higher headquarters direction and guidance; stringently controlled and time-consuming procurement/contracting processes; and dependence upon the capabilities, resources, and cooperation of many host organizations.

26.2.3. Requirements

For success under these challenging conditions the NCIS facility planning cycle, along with implementing plans and processes, must be, responsive to evolving mission requirements; systematic in formulation; disciplined in execution; and adequately flexible to take advantage of opportunities, accommodate emergent facility projects, absorb cost overruns, and cope with the changes that are inherent to any dynamic organization.

26-2.4. Integration

The effectiveness of the NCIS Facility Planning Cycle depends largely upon its successful integration with other important Navy and NCIS planning cycles. The most significant are:

a. The NCIS Strategic Planning Cycle. Produces the strategic vision statements that set NCIS course and speed for the planning years. These statements contain the direct and implied facility requirements that underpin NCIS facility plans and drive the "mission requirements" portion of the facility planning cycle.

b. The Navy Budget Cycle. Provides the financial resources necessary to staff the facility organization, operate and maintain facilities, and execute facility projects.

c. Navy Facility Planning Cycles. The Navy's Military Construction (MILCON) and Unspecified Minor Construction (UMC) planning cycles, among others, provide the means to execute facility projects that are beyond the authority and means of NCIS.

26.2.5. Facility Management Products

The NCIS Facility Planning Process results in the production of plans and other facility management products that support NCIS facility programming and execution.

a. Regional Facility Visions and Plans. Regional facility visions and plans are facility management blueprints that describes the organization, tools, training, resources, processes, strategies, and goals necessary to enhance NCIS mission capability by supporting the NCIS strategic vision.

b. Master Facility Project List (MFPL). The immediate output of the planning process is the MFPL. A comprehensive listing of all validated NCIS facility projects, the MFPL serves as the basis for annual facility programs and resource allocation decisions. The MFPL is maintained by NCIS Code 11A.

c. Annual Facility Programs. Beginning each spring the projects on the MFPL are categorized and prioritized to form the coming fiscal year's annual facility program. The annual facility program formulation process includes:

(1) NCIS Code 11A development of a proposed annual facility program with recommended project categories and priorities.

(2) Special Agent in Charge (SAC) and Deputy Assistant Director (DAD) level staffing of the proposed annual facility program.

(3) Executive Assistant Director (EAD) and Assistant Director (AD) level staffing of the proposed annual facility program.

(4) A decision brief to the Deputy Directors and/or the Director, which results in an approved annual facility program for the upcoming fiscal year. This prioritized, costed, and fiscally unconstrained listing of all validated NCIS facility project requirements is then available for consideration during the final stages of the upcoming fiscal year budget formulation and fund allocation.

(5) Financial Management Directorate promulgates the upcoming fiscal year's facility budget. A corresponding funding "cut line" is applied to the program. The "cut line" defines the projects that are funded for execution in the coming fiscal year. Unfunded projects will be executed in priority/logical order when and if additional funding sources are identified or they will be rolled over for consideration in following fiscal year.

(6) Each annual facility program should include funding for "emergent projects." This program line provides within-budget flexibility to address un-forecasted but high priority facility projects, facility targets of opportunity, cost increases, and the execution of additional MFPL projects.

26.2.6. Facility Management Tools

a. Facility Project Request (FPR), NCIS 11012.6.1 (12-2007). The FPR is the standard NCIS form, located in the administrative forms section of the NCISnet, and should be used for requesting a facility project. When properly submitted and processed, the FPR formally documents a facility project's originator, description, justification, impact, operational validation, technical assessment, and approval. FPRs may be submitted any time of the year. They should be submitted as soon as a facility requirement is identified and the project's description, justification, and impact can be clearly delineated. It takes time for the FPR to be operationally validated, technically assessed, and for an adequate scope of work and budget-worthy cost estimate to be developed. Simple, relatively inexpensive projects can be processed in a matter of weeks. Large, complex, controversial, and/or expensive projects will likely take months to validate and develop. FPRs that emerge from the validation and development process are added to the Master Facility Project List.

b. Computer Aided Facility Management (CAFM) Program. NCIS facility records (data, documents, drawings, floor plans, etc.) are predominantly paper-based, incomplete, outdated, difficult to access, and time/labor intensive to compile. The data necessary for effective facility management, budgeting, and short-/mid-/long-term facility planning is not readily available. NCISHQ has procured the CAFM system Archibus, which is capable of managing, organizing and reporting facility data, photographs, documents, Auto-CAD drawings, floor plans, and other types of information for all NCIS facilities. Archibus will be web-based, allowing appropriate levels of access to NCISHQ, EAD Staff, and FO personnel with facility responsibilities. When fully implemented, Archibus will support NCIS's ongoing evolution into a modern, competitive naval entity.

c. Site Visits. NCISHQ and FO personnel may employ site visits to obtain first hand information on the current status of facilities. Information gaps may be filled, facility records updated, potential facility projects considered, ongoing facility projects monitored, and completed facility projects evaluated for completeness and adequacy. Updated information obtained from site visits must be entered into the CAFM Program.

26-3. ROLES AND RESPONSIBILITIES OF AGENCIES EXTERNAL TO NCIS

26-3.1. Commander Navy Installations Command (CNIC)

Provides shore installation services and support to sustain and improve current and future Fleet readiness and mission execution. CNIC provides unified and consistent procedures, standards of service, practices and funding to manage and oversee shore installation support in the full range of base operating support functions. CNIC centrally and exclusively controls the leasing of commercial space for DON usage.

26-3.2. Navy Regions

The United States and overseas areas have been subdivided into 12 Navy facilities planning areas. NAVFACINST 11010.45D is an extension of OPNAVINST 1000.16J, which establishes regions as the responsible level to carry out shore facilities planning. Regional planning broadens the base of infrastructure decision-making beyond the activity by delegating decision-making to individual regions in the new regional shore establishment. In the past, Navy planning focused on developing individual activity master plans. Regional planning recognizes the need to emphasize comprehensive planning at a regional level.

26-3.3. Naval Facilities Engineering Command (NAVFAC)

Manages the planning, design, and construction of Navy shore facilities around the world. Provides facilities engineering, scientific, architectural and technical support to the naval community through engineering field divisions and activities.

26-3.4. Base (Activity) Commanding Officer

a. Participate in comprehensive planning for thier activity with respect to the overall regional plan.

b. Manage land and facility assets efficiently to assure proper maintenance, safety and appearance.

c. Prepare Shore Base Readiness Reports as required by OPNAVINST 3501.167B and evaluate how well facilities meet mission demands.

d. Develop land and facility requirements based on mission, tasks, workload, and base loading data.

e. Assist NAVFAC Engineering Field Divisions (EFD) to determine the material condition of facility assets.

f. Maintain current base mapping and a database of land, facility, and infrastructure information.

g. Recommend planning actions, initiates project documentation preparation, structure demolition and property disposal plans.

h. Review projects with the Major Claimant.

i. Prepare site approval requests and submit to the EFD.

26-3.5. Public Works Officer (PWO) is the installation representative, reporting to Regional Engineer or Installation Commander, and is responsible for providing quality engineering and maintenance services.

26-3.6. Resident Officer In Charge Of Construction (ROICC) provides project management, oversight, and administration of construction and repair projects.

26-3.7. General Services Administration (GSA) is responsible for the acquisition and administration of leased facilities for the Department of Defense (DoD). CNIC approval is ALWAYS required prior to GSA pursuit of DON leased space.

26-4. ROLES AND RESPONSIBILITIES INTERNAL TO NCIS

26-4.1. Deputy Director for Management and Administration (DDM&A) is responsible to the Director for the provision of NCIS operating facilities and the support systems that make those facilities fully functional.

26-4.2. Geographic Executive Assistant Directors

a. Provides an operational assessment of and recommendations to facility master plans and annual facility programs.

b. Determines the operational validity of FPRs submitted by SACs within their geographic area of responsibility and provides a corresponding endorsement.

26-4.3. Operational Executive Assistant Directors

a. Provides an operational program assessment of and recommendations to facility master plans and annual facility programs.

b. Determines the operational validity of FPRs submitted by DADs and SACs within their program areas and provides a corresponding endorsement.

26-4.4. Assistant Director for Administrative and Logistics (NCIS Code 11)

a. Responsible to the (DDM&A for the provision of NCIS operating facilities, vehicles, and supply/procurement support.

b. Evaluates and endorses facility plans and budget requests.

c. Ensures that all projects with facility and Information Technology (IT) components are carefully coordinated with NCIS Code 15.

26-4.5. Assistant Director for Planning and Evaluation (NCIS Code 14)

a. Produces the NCIS strategic vision statements and plans from which facility visions and plans are derived.

b. Provides a strategic assessment of and recommendations to facility master plans and annual facility programs.

c. Evaluates FPRs for conformity to NCIS strategic plans and provides corresponding endorsements.

26-4.6. Assistant Director for Information Technology (NCIS Code 15)

a. Provides a technical assessment of and recommendations to facility plans and annual facility programs.

b. Provides a technical evaluation of FPRs that include an IT component.

c. Provides IT infrastructure requirements (cable trays, cabling, wiring, etc.), ensures that all related cost estimates are included in facility project cost estimates, and coordinates (as required) scheduling of IT infrastructure-related events.

d. Funds and ensures provision of IT user equipment (computers, telephones, printers, etc.) associated with approved and executed facility projects.

e. Ensures that all IT projects with facility components are carefully coordinated with NCIS Code 11.

f. Acts as project manager for IT projects (e.g., network upgrades) and provides full resources for project completion (to include facility components).

g. As required, conducts physical security surveys in coordination with NCIS Code 11A.

26-4.7. Deputy Assistant Director for Security and Facilities (NCIS Code1A)

a. Serves as the Facility Program Manager for NCIS

b. Drafts and maintains the facility visions and plans in support of the NCIS Strategic Vision.

c. Develops NCIS facility policy and procedures.

d. Manages the NCIS Facility Planning Cycle.

e. Provides facility advice and assistance to NCISHQ and FO personnel.

f. Develops, staffs, and submits annual facility project plans.

26-4.8. Engineering Chief, Engineering Support Branch (NCIS Code 11A)

a. Executes the Annual Facility Program.

b. Establishes detailed procedures for identifying facility requirements and initiating corrective action.

c. Monitors Facility Project Requests. Assures that validated FPRs are processed for inclusion on the MFPL.

d. Acts as project manager for facility projects and provides funding for project completion, including systems furniture and IT infrastructure components.

e. Coordinates facility projects with NCIS Code 15 for identification and funding of all communication and IT components, as appropriate.

f. Coordinates facility projects with NCIS Code 11B for identification and funding of all Class III and IV property components (furniture, equipment, supply items, etc.), as appropriate.

g. Assures that spaces comply with applicable physical security requirements.

h. Reviews and recommends approval/disapproval of all lease requests, host/tenant, and other agreements required to support the acquisition, repair, alteration, or disposal of workspaces assigned to NCIS personnel.

i. Provides facility management and engineering assistance to all NCISHQ and FO elements.

j. Maintains the Archibus Program in support of NCIS facility management, planning and budgeting efforts.

k. Oversees and supports SAC and DAD efforts to keep Basic Facility Requirement (BFR) documentation current and accurate.

26-4.9. Special Agents in Charge

a. Works directly with host organizations, such as Public Works Centers and GSA facility management offices, to ensure maintenance and repair requirements are satisfied.

b. Provides input to the annual call for facilities projects.

c. Submits FPRs as facility project requirements surface.

d. With support from the NCIS Code 11A Supervisory General Engineer, keeps BFR documentation for all facilities current and accurate.

e. Represents NCIS interests while participating in and keeping cognizant of base master planning efforts. Reports significant matters to NCIS Code 11A.

f. In consultation with NCIS Codes 11A and 11C, negotiates and reviews Memoranda of Agreement (MOA), Memoranda of Understanding (MOU)/Inter-Service Support Agreement (ISSA), , GSA leases, and other occupancy agreements with host organizations.

26-4.10. Deputy Assistant Directors

a. Provides input to the annual call for facilities projects.

b. Submits FPRs as facility project requirements surface.

c. With support from the Supervisory General Engineer, keeps BFR documentation for all facilities current and accurate.

26-5. GLOSSARY

Facility managers and facility engineers employ many technical terms in the execution of their responsibilities. Some of these terms are so fundamental to effective facilities management that they must be familiar to all NCIS personnel with facility responsibilities. For your convenience many of these terms, with working definitions, are listed in this glossary. Keep in mind that the references and other sources contain detailed and sometimes complex definitions of these terms. The staff of theEngineer Support Branch stands ready to answer questions and provide more detailed interpretations as your needs dictate.

a. Basic Facility Requirement (BFR). The BFR is a document that reflects the minimum facility features and square footage necessary for an activity to perform its mission. BFR square footage determinations are derived in a very structured and controlled manner from the activity's mission requirements, personnel staffing, special requirements, and other factors. Because BFRs drive the space assignment process, they are fundamental host-tenant documents aboard Navy and Marine Corps Bases. They must be kept current and accurate.

b. Construction. The erection, installation, or assembly of a new facility; the addition, expansion, extension, alteration, conversion or replacement of an existing facility; or the relocation of a facility from one installation to another. Construction includes equipment installed in and made an integral part of the facility, and land improvements such as site preparation and landscaping. Construction projects over established cost limits are subject to Congressional control and oversight.

c. Facility. A separate, individual building, structure, utility, or other form of real property including land owned or leased by the host activity or agency.

d. Facility Management. The practice of coordinating an organization's physical workplaces with its people and work. Facility managers integrate people with purpose and place, harnessing

the principles of engineering, architecture, finance, business administration, and the behavioral sciences to optimize the utility, quality, and economy of an organization's work environment.

e. Facility Planning Cycle. The process of identifying, prioritizing, designing, budgeting for, managing, and executing facility projects of all types.

f. Host. An organization or entity that provides facilities and services to a tenant organization or entity.

g. Incrementation. Incremetation is the prohibited practice of dividing a construction project into smaller components in order to circumvent programming and approval requirements. While this is a complex area of facility regulation, the general rule of thumb is that every construction project must result in a complete and usable facility or a complete and usable improvement to a facility.

h. Lease. Acquisition of private property outside the military perimeter for unusual cases where Navy, or other federal property, is unavailable and is considered a temporary solution while a permanent facility is programmed through the Navy's Facility Planning Cycle. Leased property is requested and approved through the Navy's Regional Commander and further processed through GSA. Rent is paid on a yearly basis from the Federal Building Fund.

i. Maintenance. The work necessary to preserve or restore a facility to a state of readiness for its designated purpose. Maintenance or preventive maintenance includes actions taken to prevent wear and tear to a facility, its mechanical systems and/or other component parts to avoid or delay replacement.

j. Maintenance of Real Property (MRP). A generic term for funding expended on improvements or repairs to real property. MRP funds are also used for minor construction projects.

k. Memorandum of Agreement (MOA) / Memorandum of Understanding (MOU)/Inter-Service Support Agreement (ISSA). An MOA, MOU, or ISSA is a written document that describes the facilities and services provided by the host command to the tenant, and establishes the host/tenant responsibilities with respect to issues of maintenance, utilities, emergency services, and payment for services by the recipient. Such agreements must be developed in accordance with NCIS Policy Document 05-06/11C-0016, Administrative Policy for Preparing and Executing MOUs/MOAs, dated 30SEP05.

l. Project. A single planned undertaking of construction, repair, maintenance and/or equipment installation satisfying a set requirement.

m. Real Property. Land (Class 1) and buildings, structures, utility systems and/or other improvements to land (Class 2). The use of MRP funds is restricted to Class 1 and Class 2 property.

n. Regional Shore Infrastructure Planning (RSIP). Regional planning broadens the base of infrastructure decision-making beyond the activity. The comprehensive RSIP process addresses land, facilities, transportation and circulation, utilities, the environment, and natural and cultural resource planning elements. In addition, the RSIP process takes a long-range view of the shore establishment; it looks into the future at socioeconomic, political, environmental, and missions issues that impact the development, use and management of the shore infrastructure. It then develops strategies and actions to improve the shore infrastructure.

o. Repair. The restoration of a facility to such condition that it may be effectively used for its designated purpose by overhaul, reprocessing or replacement of constituent parts or materials that have deteriorated by action of the elements or wear and tear in use and which have not been corrected through maintenance.

p. Tenant. A unit or activity that occupies facilities provided by a host command or activity.

CHAPTER 27
TITLE: NCIS INFORMATION TECHNOLOGY
POC: CODE 15
DATE: DEC 06

POLICY DOCUMENTS
APPENDIX (2) Gen Admin 11C-0026 of 26 July 2011 released NCIS Policy Document No. 11-14: Information Management (NCIS Web Site Consolidation and Governance) Policy document 11-14 contains revised or new policy that has not been incorporated into this chapter and should be reviewed in its entirety.

27-1. GENERAL

a. The use of Information Resources at the Naval Criminal Investigative Service (NCIS) evolved and expanded from the initial primary harnessing of PCs for Standard Systems Document (SSD) preparation to an indispensable, capable war-fighting asset. Users are empowered with the means to identify, evaluate, acquire, manipulate and manage information necessary to accomplish their operational and administrative mission. The NCIS vision is to build and evolve a secure, enterprise-wide infrastructure that enables the sharing of information across organizational boundaries. The "bottom line" ... get the right information to the right people at the right time.

b. The objective of this chapter is to provide information to safeguard, administer, control, and utilize Information Technology (IT) and Information Resources (IR) within the NCIS agency.

c. Terminology used within DOD Information Assurance is defined in Appendix (1) at the end of this chapter.

27-2. USER COMMUNITY ROLES AND RESPONSIBILITIES

a. Safeguarding of Government Assets. IT is assigned to a directorate/department/office/individual to fill a specific computer-related automation requirement. Users are to safeguard their assigned IT as they would any other high value

personal or government furnished item. Physical security requirements apply to assigned software, peripherals, and any other ancillary equipment as well.

b. Protection of Information. Security of hardware, software, communications media, and data is the responsibility of the individual user.

(1) Users must, first and foremost, **protect** any and all **passwords** assigned to them. At a minimum, users must not provide their account passwords to others and must avoid allowing others to watch when they are entering passwords. See the NCIS AIS Security Manual for other guidelines regarding password protection.

(2) Security applies not only to unauthorized disclosure of information but applies equally to the preservation of data, assurance of the quality and integrity of the data, proper backup of data for recoverability.

(3) The same security practices and procedures that are used to protect information which is stored on a hardcopy (paper) medium also apply to the same classes of information when they are stored on electronic media (e.g., diskette, CD, removable hard drive, etc.).

(4) The user is responsible to ensure appropriate security measures are in place for their respective system equipped with dial-up modem communication capability, prior to any use of such systems.

27-3. SUPERVISOR RESPONSIBILITIES

a. Supervisors are responsible for ensuring that users within their work unit are fully aware of their responsibilities towards the NCIS Information Technology and towards the data to which they have access, as well as being aware of the existing procedures for the use and protection of the IT and data in their care.

b. Supervisors will ensure that security procedures are known and followed and that all required protective measures are taken.

c. Supervisors have the additional responsibility of ensuring that procedures are in place that will ensure the availability of all critical information within their area of functional responsibility, regardless of changes in personnel or operational circumstances.

27-4. NCIS INFORMATION SUPPORT RESOURCES AND SERVICES

a. FIELD COMPUTER SPECIALISTS (FCS). One computer specialist is located at each NCIS Field Office (NCISFO). FCS personnel are part of the NCIS Headquarters (NCISHQ) Code 0015 Staff but work directly for the management of the NCISFO, performing a wide variety of functions in support of NCISFO activities. These include: development of applications; administration and support of Field Office Local

Area Networks (LANs); some degree of user training; support of computer crime investigations; assisting in software/hardware installations; maintaining software/hardware inventories in each NCISFO, etc.

b. NCIS INFORMATION TECHNOLOGY SOLUTION CENTER (ITSC) is the primary point of contact for all IT and IR problems within NCIS.

(1) NCIS personnel experiencing IR/IT problems should contact the NCISHQ ITSC directly at (C) 202-433-9330/31/32, or (DSN) 288-9330/31/32.

27-5. NCIS INFORMATION RESOURCE MANAGEMENT GUIDELINES

27-5.1. POLICY. Distribution, installation, use, and support of microcomputer hardware and software will be in accordance with NCIS policy, as set forth herein, in order to ensure accountability and conform to sound management practices.

27-5.2. HARDWARE CONFIGURATION MANAGEMENT

a. All Information Technology (IT) will be subject to centralized configuration management by Code 0015. Code 0015 will coordinate and/or monitor all distributions and installations.

b. Code 0015 Asset Manager will utilize appropriate PC tracking software to query and report on all pertinent IT asset data to include: , serial number, location, maintenance and warranty information, software tracking and license utilization, and person/code assigned. The Asset Manager will assist and train the FCS in ensuring a complete inventory data baseline of IT assets under their control.

(1) The individual/supervisor to whom the IT is assigned will be personally responsible for the proper use, upkeep and care of the IT.

(2) It will be the responsibility of the individual supervisor, to turn in assigned IT and/or notify Code 0015 of the need to re-assign IT assets upon detachment of the individual/ supervisor.

c. Without exception, personally-owned computers(non-NCIS) are not authorized.

27-5.3. COMMERCIAL OFF-THE-SHELF-SOFTWARE

a. NCIS personnel use a variety of Commercial Off-The-Shelf (COTS) software packages. However, because there are so many COTS packages on the market, it is not possible for NCIS personnel to be familiar with and/or support all the different types of packages that provide the capability to perform any given function.

(1) When a COTS package is determined to meet the need of an operational requirement, the respective office (or, code) is required to request permission for the COTS to be installed. Code 0015 follows strict configuration management rules.

(2) Most COTS software is copyright protected and must not be duplicated.

27-5.4. COMMUNICATIONS STANDARDS

a. Wide Area Network (WAN) communications are accomplished using Department of Defense (DOD) Communications Networks.

(1) No element of the NCIS is authorized to obtain communications services without coordination with Code 0015, who will, in turn, coordinate with Navy and DOD communications authorities.

(2) Unless NCIS has obtained specific authorization from DOD approval authorities, NCISHQ elements may not contract for purchased communications services.

27-6. MANAGEMENT OF INFORMATION AS A RESOURCE

27-6.1. AUDITS AND INSPECTIONS. As with any "tool" which management furnishes to employees for the conduct of business, once IR policy has been defined, users must be held accountable for compliance, and follow-up inspections or audits must be held.

a. Periodic audits/inspections will be conducted in conjunction with NCISHQ and NCISFO inspection requirements.

(1) On request, Code 0015 will furnish to the inspection team, hardware, and software inventories to include serial numbers, nomenclature, and standard and/or individual configurations as may be appropriate.

(2) NCISFO inspections may serve as a preliminary evaluation allowing a "management re-direction" where appropriate, prior to formal compliance evaluation.

b. After the results of audits and inspections have been received, policies, procedures, performance measures and user training methodologies should be reviewed and re-evaluated. Wherever necessary, changes, revisions and innovations should be considered, formulated, validated and promulgated.

27-7. NCIS INFORMATION SYSTEMS SECURITY PROGRAM

27-7.1. INTRODUCTION

a. SECNAVINST 5239.3 and the Naval Information Assurance Publications (NAV IA Pubs) provide procedural, technical, and administrative guidance for all Information Systems, whether business or tactical, used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data.

b. NCISINST 5239.1A (28 June 1994), currently being revised and in draft form, is the current Information Security (INFOSEC) instruction being implemented NCIS-wide. This instruction provides detailed information and should be referred to for information within specific subject areas.

c. All data (including Privacy Act, "For Official Use Only", sensitive criminal investigative data, etc.) must be protected and its integrity insured.

d. An effective INFOSEC program requires that the following security objectives be met:

(1) Confidentiality of personal, proprietary or otherwise sensitive data handled by the system; and,

(2) Integrity and accuracy of data and the various authorized processes that handle the data; and,

(3) Availability of systems and the data or services they support.

e. A wide range of events and conditions can adversely affect reaching sound objectives. These include, but are not limited to:

(1) Lack of awareness or concern for the implications of computer security issues; and/or,

(2) Carelessness, errors or omissions; and/or,

(3) Equipment and media failure hazards; and/or,

(4) Intentional attacks by disgruntled or dishonest personnel, hackers or hostile agents.

f. The various manifestations of each type of threat are limited only by the specific characteristics of the system, data and operational environment.

27-7.2. ROLES AND RESPONSIBILITIES

a. Designated Approving Authority (DAA). The DAA is the official who decides whether an AIS network or computer resource may operate. The Director, NETWARCOM, is the DAA for most systems located at NCISHQ and NCISFO.

b. Information Assurance Manager (IAM). (IAM is interchangeable with numerous acronyms throughout DOD and DON.) The IAM is appointed in writing and has the responsibility to manage and implement the AIS Security Program that includes the accreditation of computer systems and maintaining a risk management program. The IAM for NCIS is located in Code 15I.

c. Information Assurance Officer/System Administrator. An IAO or System Administrator will be appointed for each information system used to process classified data and sensitive unclassified data requiring special protection (i.e., Privacy Act, For Official Use Only). The IAO will be the focal point for all AIS security matters for the assigned system of responsibility.

27-7.3. MINIMUM SECURITY PROGRAM REQUIREMENTS. The following terms represent and define areas where minimum security requirements exist. Refer to NCISINST 5239.1 for detailed requirements. The following is a brief description of these requirements:

a. Access Control. Each information system resource requires an automated or affixed warning banner. The banner should identify the resource as a protected government system and continuation of the log-on consents to monitoring.

b. Accreditation. A review of the security posture of the total AIS environment is conducted and the DAA for that system issues an accreditation letter that makes a formal declaration that all appropriate security measures have been effectively implemented and that an adequate level of security has been achieved.

c. Classified Processing. The requirements to process classified information are too numerous to describe in detail in this chapter and reference must be made to NCISINST 5239.1, as well as NISCOMINST 5510.1H, and SECNAV 5510.36.

(1) Classified information is not permitted to be processed on a PC connected to an unclassified Local Area Network (LAN) under any circumstance. It is forbidden to insert a classified disk into the drive of an unclassified computer (PC), or, to view, modifying, etc., any files on that disk.

(2) In the event classified processing is authorized to occur on a fixed hard drive – and, the information authorized to be stored on that hard drive - approval for open storage must be obtained from the NCIS Security Manager, or, the media must be safeguarded in an approved GSA security container.

d. Color Coding. Magnetic media and electronic storage components will be color-coded: green for Unclassified media; blue for Confidential media; red for Secret media; and, orange for Top Secret media.

e. Configuration Control. If a configuration change is going to occur which may alter the security posture of an information system resource, approval must be obtained by the DAA or ISSM.

f. Controlled Access Protection (CAP). CAP is an established set of controls to help protect information from unauthorized disclosure, modification, destruction and/or loss.

g. Copyright Protection. Usually, a COTS package is a proprietary product of the company that developed the product, and protected by U.S. copyright law.

(1) Each licensing agreement that is included with a software package contains express guidelines for the authorized use, copying, and modification rights granted to the user.

(2) Any use of such software beyond the rights specified in its licensing agreement is prohibited by federal statutes as well as by DON regulations.

i. Data Integrity. Data within an information system resource will have an identifiable origin. In addition, its use, accessibility, maintenance and disposition will be governed on the basis of its classification, its sensitivity, and the users' need-to-know, and other restrictions.

j. Declassifying Automated Information System Media.

(1) Clearing techniques (i.e., overwriting once with approved software) are used when media will remain in the facility with the expectation of being reused. Cleared Automated Information System (AIS) media is required to be marked, safeguarded and controlled at the highest level of classification recorded on the media, before being cleared.

(2) Purging techniques are used when the media will be released outside the facility, i.e., sent out for repair, or released for reutilization at another facility.

(a) Confidential and Secret may be purged by overwriting three times with approved software, or, degaussing.

(b) Top Secret is purged by degaussing.

(c) Purged media retains its classification until removed administratively.

k. Emanation Security. All information systems resources processing classified information will comply with TEMPEST Program requirements as given in OPNAVINST C5510.93 and OPNAVNOTE C5510 dated 14 April 1994.

l. Freeware/Shareware. Use of freeware/shareware is discouraged. However, if it is required, shareware will be legally purchased and the distribution/usage limitations will be respected at the same level as for a commercial software copyright.

m. Incident Reporting. Incidents involving loss, possible compromise or actual compromise of classified information should be immediately reported to Code 15I, the IAO/System Administrator, IAM and/or the NCIS Security Manager, as appropriate.

o. Passwords. All passwords, whether used for access control or authentication purposes, will be changed every ninety days or immediately upon suspicion of compromise.

p. Privately Owned Resources. **Privately owned information resources MUST NOT be used to process classified information.** The government assumes no liability for privately owned resources. In addition, an agreement will be signed by the owner, supervisor and IAM/DAA to indicate approval for use of the privately owned resource.

q. Storage of Magnetic Media. Magnetic media will be stored in accordance with the requirements for hardcopy of like sensitivity and classification.

r. Use of government Information Resource (IR). All government owned IR is required to be used for official U.S. government business only. Additionally, no classified information will be processed while the resource is outside government spaces without express written permission from the NCIS Security Manager.

s. User Agreements. Each employee who uses, or, has access to an Information Resource, will sign a security agreement DD Form 2875 (APR 2005) agreeing to abide by established policy. The most current user security agreement is posted on the Infoweb.

t. Virus Protection. All media will be checked for known malicious codes/viruses before being used with any government owned Information Resource. Memory-resident scanning software will be used to the maximum extent possible.

u. Waivers. Deviation from the established policy must be officially requested through the chain of command from the IAM, Security Manager, or DAA as appropriate. The request will be evaluated and a recommendation of acceptance or rejection will be forwarded to the Director, DAA or higher authority, as appropriate.

v. Welcome Banners. Sign-on screens that reflect the System name, the type of data will not be displayed by AIS or any other IR until the user and the user's authorization is authenticated and verified.

27-7.4. GENERAL SECURITY GUIDELINES. Some common-sense protective measures can reduce the risk of loss, damage, or disclosure of information. The following

are the most important areas, but not limited to, of information systems controls that assure the system is properly used, resistant to disruptions, and reliable.

a. Security Awareness. All users should treat information as a valuable asset. Just as users would not walk away from their desk leaving cash or other valuables unattended, users should take the same care to protect information. Users unsure of the value or sensitivity of the various kinds of information they handle should ask their supervisor for guidance. All users must take the Information Assurance Awareness course prior to receiving access or an account to any NCIS network to include Non-Secure Internet Protocol Routing Network (NIPRNet), Secure Internet Protocol Routing Network (SIPRNet) and Joint Worldwide Intelligence Communication System (JWICS).

b. Password Security. The user should make certain no one can "impersonate" them. Although a login ID initially identifies a user, a password is used to verify that user's identity. Thus, passwords are a significant element of system security.

(1) Do not disclose passwords to anyone, or allow anyone to observe passwords as you enter them during the sign-on process.

(2) Each user must change their password every 90 days. Periodic password changes make it harder for unauthorized users to gain access to information systems by "borrowing" the password of a legitimate user.

c. Authorized Use. Government computer systems are only to be used for lawful and authorized purposes.

(1) Use of NCIS computers and computer systems is restricted to authorized users.

(2) DOD computer systems, including NCIS systems, are provided for the processing of official US government information only.

(3) The use of Information Technology is restricted to those functions that are necessary to carry out job responsibilities.

(4) Systems may be monitored to ensure information security, system integrity, and the limitation of use for official purposes.

(a) The use of NCIS computers and computer systems constitutes consent to monitoring, interception, recording, reading, copying, and capturing of any of the data in these computers and computer systems as an integral part of the system management.

(b) Information derived from system monitoring may be used as a basis for administrative, disciplinary, or criminal proceedings.

d. Observe Established Policies and Procedures. The DOD, DON and NCIS established specific requirements for the protection of information in policy manuals, rules and procedures.

(1) General guidance is located in: DCID 1/16, DIAM 50-4, DATE 5200.1, DOD 5200.1R, DOD 5200.28, SECNAVINST 5239.2, OPNAVINST 5510.1H, NISCOMINST 5510.1H, NISCOMINST C5500. 6, National Computer Security Center (NCSC) Rainbow Series, NCIS-1 Manual and other specific resources as applicable.

(2) Users should ask their supervisor if they are unsure about responsibilities for protection of information.

e. Personal Accountability. After authorization to use a computer system has been granted, users become personally responsible and accountable for their activity on the system.

f. Anti-Virus Precautions. In the past, NCIS has been affected by computer "viruses" acquired through seemingly useful or innocent software obtained from public access bulletin boards or other sources.

(1) Since the installation of unauthorized hardware can cause damage, invalidate warranties, or have other negative consequences, only hardware or software that has been acquired through normal acquisition procedures and that complies with all software licensing agreement requirements will be installed.

(2) Business-related electronic information brought into the organization for use will be filtered through the IT representative for review prior to being utilized on any system.

(3) All diskettes, files and/or software brought in from outside the organization must be subjected to virus scanning programs prior to use on any NCIS equipment.

g. Report Anomalies. Report all unusual or questionable occurrences to your supervisor, FCS, or Information Assurance Branch, Code 15I.

(1) Many losses could be avoided if computer users report any circumstances that seem unusual or irregular.

(2) Warning signals could include such things as unexplainable system activity that you did not perform, data that appears to be of questionable accuracy, and unexpected or incorrect processing results.

27-8. INTERNET USAGE BY NCIS PERSONNEL

27-8.1. NCIS INTERNET USAGE POLICY AND SECURITY GUIDELINES

a. INTERNET Usefulness. The usefulness of INTERNET to NCIS lies in the access and capabilities described above. This access and these capabilities will serve both the administrative and operational interests of NCIS.

b. Importance of Controls.

(1) Risk Factors. The prime advantage of INTERNET (the ability to communicate with virtually anyone, anywhere) is also the characteristic that presents the greatest risk to NCIS. After all, without stringent controls, access can be made to work both ways, whether or not such was originally intended.

(2) Minimizing these risks to NCIS, to its users, and to its information, is paramount. Therefore, it is important to establish controls over the use, administration and operation of both the NCIS INTRANET System and Public INTERNET System(s).

(a) The NCIS INTRANET System (NCIS version of the INTERNET system) will allow access to information controlled by an NCIS INTERNET System Administrator (ISA), contained within an NCIS-only environment, and exchanged only among NCIS users.

(b) The Public INTERNET (the internationally recognized network system to which that term commonly refers) will allow NCIS personnel to access external information networks and information sites - whether they originate from government or business sources - to which NCIS has subscribed, to which access is open, and/or to which access has been otherwise legitimately obtained by an NCIS administrator.

(c) NCIS users access the INTERNET in one of two ways - by means of the NCIS Network through a "Firewall" device, or by means of a standalone PC and a communications modem using a commercial service. Any NCIS unit opting for the 'stand-alone' approach will also have to absorb the costs of that approach.

(3) It is imperative for the NCIS user to thoroughly understand the established and required standards, guidelines and security controls before being granted access to the INTERNET or authorized entry into the NET.

(4) The NCIS user is required to adhere to the established NCIS policy guidelines and procedures for INTERNET access and usage.

27-8.2. RESPONSIBILITIES

a. NCIS established the following guidelines for use of the INTERNET: all employees are expected to read and comply with the enclosed statement of policy; and, violations of any of the rules, established in this attachment may be used as a basis for adverse administrative and/or disciplinary action.

b. The INTERNET is not a single network; rather, it is a group of thousands of individual networks allowing traffic to pass among them. The traffic sent out to the INTERNET may actually traverse several different networks before it reaches its destination. It is essential for each user to recognize their responsibility in having access to these vast services, sites, systems, and people. The user is ultimately responsible for their actions in accessing the INTERNET.

c. Use of the INTERNET is a privilege, not a right. Access to the INTERNET may be revoked at any time. Access is provided to the user as a business tool to enhance productivity in the following:

(1) Directed NCIS research; and/or,

(2) Access to vendor information for support of products owned by NCIS; and/or,

(3) E-mail communication with clients or vendors.

The user is responsible for using the INTERNET services in a manner consistent with NCIS' commitment to the highest business and ethical standards. The following are examples of inappropriate INTERNET usage:

- Accessing any pornographic material or material that negatively depicts race, sex or creed.
- Sending any message that may be perceived as threatening.
- Sending racially and/or sexually harassing messages.
- Posting statements or information about NCIS, or data for which NCIS is responsible, except with written approval by the Director or a Designated Authority.
- Conducting personal research or any use of the INTERNET for personal gain.
- Giving anyone else use of your account.
- Accessing chat facilities for personal use.
- Sending chain letters.
- Copying electronic files without permission.
- Violating copyright laws.
- Using NCIS equipment or resources to violate any law or perform any unethical business acts.
- Performing unauthorized attempts to break into any computer, unless in the performance of an audit authorized by senior management.
- Playing games.
- Establishing any connection from the INTERNET or service provider into any NCIS system, equipment, etc., unless specifically authorized, in writing, by the Director or Designated Authority.
- Sending or posting confidential materials to any unauthorized people, inside or outside NCIS.

- Sending sensitive or confidential messages.
- Releasing viruses, worms, Trojan horses, or similar programs.
- Taking deliberate actions to make a computer system or network unavailable to other users.

d. General Guidelines:

(1) The user is responsible to adhere to established security procedures, including the security of their account password and not bypassing security controls. The user will be held responsible for their account use or misuse.

(2) All messages composed, sent or retrieved via NCIS' INTERNET connection are NCIS property, and may be reviewed at any time.

(3) Mail on the INTERNET is NOT SECURE. Never include anything in an E-mail message that is sensitive or confidential.

(4) Actively disclaim speaking for NCIS. If you use your NCIS INTERNET account to post an item, NCIS' name is carried along with what you post via the domain name.

APPENDIX (1): TERMINOLOGY USED WITHIN DOD INFORMATION ASSURANCE

Access Control. A fundamental component of Information System Security procedures, protecting not only Information, but also Information Resources by regulating an individual's ability to use any element (i.e., hardware, software, information, communications, etc.) of an Automated Information System (AIS).

Acceptable Level of Risk. A judicious and carefully considered assessment by the appropriate designated approving authority that automated information systems resources meet the minimum requirements of applicable security directives and the provisions of the resource, threats and vulnerabilities, safeguards and their efficiency in compensation for vulnerabilities, and operational requirements.

Accountability. The property that enables activities on an automated information system to be traced to individuals who may then be held accountable for their actions.

Accreditation. The formal management authorization for operation of a specific system, network, Information Resource based on the results of a security certification and risk assessment. It is a formal declaration by the designated approving authority that a system is approved to operate in a particular security environment meeting a prescribed set of security requirements.

Antiviral Program. A software program developed for the purpose of identifying, detecting and notifying users of malicious code and which provides guidance for restoring all infected resources.

Assurance. A measure of confidence that the security features and architecture of an automated information system accurately mediate and enforce security policy. If the security features of an information system are relied on to protect classified information or sensitive unclassified information and restrict user access, the features must be tested to ensure that the security policy is enforced and may not be circumvented during system operation.

Audit. An independent review and examination of system records and activities to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, and to recommend any indicated changes in controls, policy or procedures.

Audit Trail. A chronological record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of events and activities surrounding or leading to an operation, a procedure or an event in a transaction from its inception to final results.

Category. A grouping of classified or sensitive information to which an additional restrictive label is applied for signifying that personnel are granted access to the

information only if they have formal access approval or other applicable authorization (e.g., proprietary information, for official use only, compartmented information).

Certification. The formal technical evaluation of security features and other safeguards made as part of, and in support of, the accreditation process which established the extent that a specific application of an information systems resource meets a set of specified security requirements.

Classified Data/Information. Information or material owned by, produced for, or under the control of, the United States government which is determined by Executive Order 12356, or, prior orders, to require protection against unauthorized disclosure.

Clear. Removal of sensitive and/or classified data from an information system at the end of a period of processing, including storage devices and other peripheral devices with storage capacity, in such a way that there is assurance proportional to the sensitivity of the data, that the data may not be reconstructed by normal or non technical means.

Commercial Off-The-Shelf (COTS) Software. Software produced by and publicly sold by a commercial vendor.

Communications Security (COMSEC). Protection of communication and telecommunications systems to prevent unauthorized disclosure and to ensure authenticity of the communication.

Compromising Emanations. Unintentional replay of intelligence-bearing signals, which, if intercepted and analyzed, disclosed the classified information, transmitted, received, handled, or otherwise processed by any information processing equipment. Tempest is the unclassified short name referring to the investigations and studies of compromising emanations.

Computer Incident Response Team (CIRT). An organization created to assist a defined constituency in reporting and handling vulnerabilities and incidents in information systems resources.

Computer Security. Measures and controls that safeguard or protect computers and the data they process against unauthorized (accidental or intentional) disclosure, modification, destruction, and denial of service. Computer security includes consideration of all hardware and/or software functions, characteristics, and/or features; operational procedures, accountability procedures, and access controls at the central computer facility, remote computers and workstations; management constraints; physical structures and devices; and personnel and communication controls needed to provide an acceptable level of risk for the computer and for the data and information contained in and processed by the computer.

Contingency Plan. A plan for emergency response, backup operations, and post-disaster recovery, maintained by an activity as part of its information systems security program.

A comprehensive statement of all planned actions to be taken before, during and after a disaster or emergency condition including documented, tested procedures which will ensure the availability of critical computer resources and which will facilitate maintaining the continuity of operations in an emergency situation.

DADMS. Department of the Navy Application and Database Management System. DADMS is a web-enabled registry of IT applications and systems and their associated data structures and exchange formats. It supports the DON in the reduction of legacy applications, the development of standard applications, databases, and data elements. It also support IT interoperability, Information Assurance assessments, and the construction and maintenance of functional and enterprise architectures. Any systems or application used within the DON must be recorded and approved in DADMS prior to being installed on any Navy network and/or computer.

Data Integrity. The state that exists when data is unchanged from its source and has not been subjected to accidental or malicious modification, unauthorized disclosure or destruction.

Data owner. The authority, individual or organization that has original responsibility for the data by statute, executive order or directive.

Degauss. The reduction of the magnetic induction of an information systems resource to zero by applying a reverse magnetizing field. Also referred to as "demagnetizing."

Denial of service. Action or actions that result in the inability of an information system or any essential part to perform its designated mission, either by loss or degradation of operational capability.

Designated Approving Authority (DAA). The official who has the authority to decide that an information systems resource may operate based on an acceptable level of risk considering the operational need for and threats to the resource and is responsible for issuing an accreditation statement that records the decision.

Emanations. Electromagnetic field existing outside an information systems resource resulting from the operation of the system.

Evaluated Products List (EPL). A documented inventory maintained by NSA of equipment, hardware, software, and/or firmware that have been evaluated against the evaluation criteria found in DODD 5200.28 Std.

FAM. Functional Area Managers are appointed by the DON and are authorized to direct the migration, consolidation, or retirement of applications and database within their respective functional areas. They are also responsible to ensure that technology strategies/systems/applications are aligned with business processes and war fighting strategies.

Formal Access Approval. Documented approval by a data owner to allow access to a particular category of information.

Freeware. Software not protected by copyright laws and therefore free for all to reproduce and trade without fear of legal prosecution for non-submission of monetary, or, other contribution, to the author or acknowledgment.

General Service (GENSER). Programs for the protection of classified material developed in accordance with basic statutes and executive orders governing the secrecy of national defense information. Excluded are specialized security programs such as Sensitive Compartmented Information (SCI) and Special Access Programs (SAP), which are governed by different directives or statutes, which go beyond or replace basic classified information protection requirements.

Hacker. A person who penetrates, in an unauthorized manner, an information systems resource, or, attempts to circumvent the security features of an information systems resource.

Information Security. A system of policies and procedures for identifying, controlling, and protecting from unauthorized disclosure, information whose protection is authorized by executive order or statute.

Information Systems Resource. All resources related to information systems and their management, including personnel, equipment, funds, and technology.

Information Systems Security Officer (IAO). Trained individual responsible for ensuring that security is provided for and implemented throughout the life cycle of an information system.

Interim Authority to Operate (IATO). A provisional statement granted by the designated approving authority for a period not to exceed one year to provide for the operation of an information systems resource pending determination that the resource has attained an acceptable level of risk.

Keyboard attack. Data scavenging through resources available to normal system users, which may include advanced software diagnostic tools.

Life Cycle Management (LCM). A standard management discipline for acquiring and using information systems resources in a cost-effective manner throughout the entire life of the information system.

Magnetic Remanence. A measure of residual information remaining on data storage media after use of insufficient purging procedures. It is also used synonymously for data remaining on magnetic media after removal of power.

Malicious Code. Code that covertly replicates itself onto media, with or without initiation by the operator, or authorized users. Replication usually occurs during copying of files to magnetic media or during computer-to-computer communications. The code usually contains logic that is triggered by some predetermined event. When triggered, the code then takes a hostile action against the resource. Several common malicious codes are:

1. Logic bomb - malicious code that is executed at appropriate and/or periodic times in the operation of an information systems resource as a result of a sequence of logical steps in the legitimate execution of a program. For instance, one type of logic bomb is a time bomb. The program continually checks the system clock and date and once a specified date/time is reached, the malicious program is executed.

2. Stealth/encrypted virus - malicious code that hides itself from all attempts to read and/or detect the code, or, returns to the screen only that data which would appropriately be viewed by the user if the malicious code were not present. These types of viruses are the most difficult to detect and/or locate thus possessing potential for grave damage to an information systems resource.

3. Trap door - set of special instructions that enable knowledgeable users to bypass security features and gain unauthorized access to information systems resources.

4. Trojan horse - a computer program that overtly changes or adds instructions or logic before executing and thus changes the execution of legitimate program sequences. A Trojan horse may also misrepresent itself to entice the user to execute it.

5. Worm - a computer program that exists, executes, and duplicates without the assistance of any other legitimate or unauthorized code. Worms generally search out unused capabilities and capacities within an Information Systems Resource to use for their own purpose, which quickly disables the resources and makes them unavailable for authorized processing.

Need-to-know. A determination made in the interest of the U.S. National Security by the custodian of sensitive, or, classified, information that a prospective recipient has a requirement for access to, knowledge of, or possession of the information, to perform official tasks or services.

Network. The interconnection of two or more independent information systems resources that provides for the transfer or sharing of computer system assets. It is composed of a communications medium and all components attached to that medium whose responsibility is the transfer or sharing of information. Such components may include, but are not limited to, information systems, packet switches, telecommunications controllers, key distribution centers, and technical control devices configured as local area networks, wide area networks, global area networks, etc.

Object. A passive entity that contains, or, receives, information, i.e., records, blocks, pages, segments, files, directories, directory files, and programs, as well as bits, bytes, words, fields, processors, video displays, keyboards, clocks, printers, network nodes, etc.

Overwrite. The removal or destruction of data recorded on an information systems resource storage media by recording patterns of unclassified date over or on top of the data originally stored on the media.

Physical Security. Measures designed to safeguard personnel, prevent unauthorized access to equipment, installations, material, computer media and documents, and to safeguard against espionage, sabotage, damage, and theft.

Purge. The process of removing classified and/or sensitive unclassified information from computer storage devices in a manner, which gives assurance proportional to the sensitivity of the data that the information will be unrecoverable by technical means. Clearing will not purge information from storage.

Risk. A combination of the probability that a threat will occur, or, the probability that a threat occurrence will result, with an adverse impact, and the severity of the resulting adverse impact.

Risk Assessment (RA). An analysis of information systems resources, vulnerabilities, and threats, to determine the security requirements that must be satisfied to ensure the system can be operated at an acceptable level of risk.

Risk Management Program (RMP). A process through which undesirable events can be identified, measured, controlled, and prevented to effectively minimize their impact or frequency of occurrence. The fundamental element of risk management is the identification of the security posture, i.e., the characteristics of the functional environment form a security prospective. Risk management identifies the impact of events on the security posture and determines whether or not such impact is acceptable, and if not acceptable, provides for corrective action. Risk assessment, security test and evaluation and contingency panning are parts of the risk management process.

Safeguards. The protective measures and controls prescribed to meet the security requirements specified for an information systems resource. Safeguards may include, but not limited to hardware and software security features, operational procedures, accountability procedures, access and distribution controls, management constraints, personnel security and physical structures, areas, and devices. Previously referred to as countermeasures.

Security Test and Evaluation (ST&E). An examination, analysis, and actual test of the security features and safeguards of an information system as they have been implemented in an operational environment to develop factual evidence upon which an accreditation can be based.

Sensitive information. Within the Naval Criminal Investigative Service, the definition of "sensitive unclassified" (referred to as "sensitive") information is interpreted as:

1. Financial information: all financial/managerial accounting activities and planning documents, including, but not limited to, accounts payable/receivable, budget submissions/approvals and payroll.

2. Criminal investigative.

3. For official use only: all information relating to an agency's public business transactions including organization, policy, function, decision, and procedure data.

4. Privacy act information: any information whose misuse could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual. Exemptions (such as name, grade or position, date of grade, gross salary, present and past assignments, future assignments if officially established, and office telephone number) and more specific information are contained in 5 U.S. Code 552(e)(10).

5. Security posture information - information relative to an agency's risk management program; including risk assessments, security tests and evaluation, contingency and security plans and accreditation schedules; site-specific configuration of security resources, equipment, systems and personnel supporting the research.

6. Other information - any other information (as identified by the information systems security officer or other security officials, legal counsel, public affairs office or any U.S. government department or agency) the loss, misuse or unauthorized access to or modification of which could adversely affect the U.S. national interest, the conduct of DON programs, or, the privacy, or, DON personnel (e.g., Freedom of Information Act exempt information and information whose distribution is limited by OPNAVINST 5510.61, withholding of unclassified technical data from public disclosure) [Public Law 100-235].

Shareware. Software that is not legally copyrighted and may be openly distributed. However, if retained, a nominal fee must be paid to the author. There are usually additional requirements such that the software may not be altered or used in conjunction with or embedded into software that will be sold for profit or nonprofit.

Special Access Program (SAP). Any program imposing need-to-know or access controls beyond those normally required for access to Confidential, Secret, or Top Secret information. Such a program includes, but is not limited to, special clearance of investigative requirements, special designation of officials authorized to determine need-to-know, or special lists of persons determined to have a need-to-know.

System of records. A group of records from which information "is," as opposed to "can be," retrieved by the name of the individual, or by some identifying number, symbol, or other identifying information uniquely assigned to the individual.

Telecommunications. Any transmission emission, or reception of signs, signals, writing, images, sounds, or information of any nature, by wire, satellite, radio, optical or other electromagnetic systems.

Tempest. An unclassified short name referring to investigations and studies of compromising emanations. It is sometimes used synonymously for the term "compromising emanations" (e.g., Tempest tests, Tempest inspections).

Threat. Any circumstance or event with the potential to cause harm to an information system resource in the form of destruction, disclosure, and modification of data, or denial of service. A threat is a potential for harm. The presence of a threat does not mean that it will necessarily cause actual harm. Threats exist because of the very existence of the resource and not because of any specific weakness. For example, the threat of fire exists to all computer facilities, regardless of the amount of fire protection available.

Trusted products. Products evaluated and approved for inclusion on the Evaluated Products List.

Unclassified information. Information that needs to be safeguarded against disclosure, but must be safeguarded against tampering, destruction, or loss due to record value, utility, replacement cost, or susceptibility to fraud, waste, or abuse.

Vulnerability. A weakness in the physical layout, organization, procedures, personnel, management, administration, hardware, or software that may be exploited to cause harm to the information systems resources. The presence of vulnerability does not in itself cause harm. Vulnerability is merely a condition or set of conditions that may allow the resource to be harmed by an attack.

APPENDIX 2

127484 13:17 20110726 IN:SSDEMAIL #28753 OUT:NCISHQWWSSD #245

GENERAL ADMINISTRATION 26JUL11

FROM: 0000 GEN: 11C-0026

TO: DIST

SUBJ: NCIS POLICY DOCUMENT NO. 11-14: INFORMATION MANAGEMENT (NCIS WEB SITE CONSOLIDATION AND GOVERNANCE)

REF: (a) Gen Admin/11C-0002/6 February 2009/NCIS WEBSITE GOVERNANCE POLICY

1. This policy document cancels reference (a).

2. For many years, NCIS maintained Web sites on NIPRNet, SIPRNet and JWICS. Each of these Web sites has different targeted audiences. The NCIS public Web site (www.ncis.navy.mil) is intended for general public consumption; the NCIS public Intelink sites on SIPRNet and JWICS are directed to Department of Defense (DoD) and Navy communities; and the NCIS NCISnet (Infoweb), NMCI SharePoint and intranets on SIPRNet and JWICS are intended for internal consumption. All the NCIS Web sites should be viewed as information and knowledge sharing capabilities that must be kept current with the most accurate information. Historically, it has been a difficult task to maintain current content and emerging technology. In 2010, Codes 15 and 00C deployed a completely revamped NCIS public Web site using SharePoint 2007. Code 15 is aggressively working to deploy a NIPRNet internal SharePoint site, which will consolidate the NCISnet (Infoweb) and our NMCI SharePoint. The NMCI SharePoint is scheduled for shutdown by the end of September 2011. The new NCIS SharePoint environment will provide many new capabilities and leverages the opportunity for a more cohesive place for communication and collaboration. SIPRNet and JWICS SharePoint implementations will occur after BRAC relocation to Quantico.

3. The new NIPRNet SharePoint Web site - known as Lighthouse - will provide a centralized location for users to store, disseminate and share information across the agency. Lighthouse will bring a variety of capabilities including document libraries, calendars, tasks, blogs, wikis, collaboration sites, discussion forums and others. Lighthouse will be the central stop for access to all NCIS enterprise applications and to reach directorate-, department- and field-level organizational information. All NCIS employees will be able to access Lighthouse. The site is hosted by NCIS on our NIPRNet network and users will be able to gain access to the site via username and password or a Common Access Card.

4. To ensure proper standards for this new environment, a governance process will be established. The purpose of the governance board is to create, arbitrate, review and oversee the policies, technology, content

maintenance structure, communication, and training efforts related to NCIS Web sites. The governance board is responsible for resolving issues, considering proposals and change recommendations, advocating resources, and motivating stakeholders. The governance board members shall include Assistant Directors from each directorate. The Assistant Director for Code 15 will serve as the chairman of the governance board. As required, Deputy Assistant Directors and special agents in charge may be asked to participate in the governance board.

5. Lighthouse is built upon four organized tiers.

a. Tier One - My Site. This tier is used by each person in the organization. It is a location where individual employees can store documents, content, links, pictures, contacts, collaborate on products, blogs, or connect with peers (share information about yourself and your skills/interests/projects, etc.). The employee controls what information is shared with whom. My Site is intended to be used as your personal shared drive. Network shared drives will be eliminated as personnel migrate their information to Lighthouse.

b. Tier Two - Team Sites. This tier provides an internal site for communication and collaboration within a team, division, or branch. The capabilities include workspaces, calendars, document libraries, task lists, discussion/collaboration, announcements and more. Access is restricted by members of the respective team. Team sites can be established for a special project or operation. User permissions will be managed by the local content administrators. They are intended to be used as the central shared location for all content which currently exists in network shared drives. Network shared drives will be eliminated as departments migrate their shared information to Lighthouse.

c. Tier Three - NCIS Shared Sites. This tier provides an internal site for communication and collaboration to the entire NCIS population from a team, directorate, department or field element. The capabilities include workspaces, calendars, document libraries, task lists, discussion/collaboration, announcements and more. Access to NCIS shared sites will be unrestricted for all NCIS authenticated users. Information from team sites may be published here for access by all NCIS employees.

d. Tier Four - Top-level (home) shared areas. This tier provides general common areas where content is combined or rolled up from other tiers. This includes announcements about NCIS, contacts, News to You, Web site links, manuals, forms, etc. Each of these areas will need to be specifically identified and authorized by the governance board and implemented by Web site and content administrators.

6. The IT Web site administrators (Code 15) are responsible for maintaining the technical infrastructure; upgrading technology; monitoring; design and specification standards; monitoring and analyzing web statistics; assessing and monitoring risks; training content administrators; and identifying issues or changes that require resolution.

Code 15 will designate two or more personnel to support web technology related to all of the NCIS Web sites.

SUBJ: NCIS POLICY DOCUMENT NO. 11-14: INFORMATION MANAGEMENT (NCIS WEB SITE CONSOLIDATION AND GOVERNANCE)

7. The departmental/office Web site content administrators are responsible for the day-to-day content for their respective office or code. They are responsible for updating, promoting and removing content from their respective shared sites; advocating and motivating their respective communities of users; managing user access to their respective sites; identifying issues or changes that require resolution; and identifying risks, issues and proposals to the Web site administrator. Any issues that cannot be resolved by Code 15 shall be submitted to the governance board for resolution.

8. Each NCIS directorate and field office shall designate two personnel who will be responsible for managing content for the NCIS intranets (NIPRNet and SIPRNet). Code 00C will designate one person who will be responsible for all public (NIPRNet) web content. Code 25 will designate two personnel who will have the responsibility for maintaining the content on all public Intelink (SIPRNet and JWICS) sites. Many offices are already performing this function within their respective departments/offices and while it should not be viewed as a full-time position, this responsibility is critical in ensuring that relevant and current information is placed in the shared areas of the web sites. Given the critical nature of the responsibility, designated website content administrators shall have a critical element added to/included in their Performance Plans that cover these responsibilities. Please submit the names of the designated Web site content administrators to (b)(6) (b)(6) @navy.mil), Code 15A, by 1 August 2011. This administrative responsibility formalizes the process to ensure that relevant and up-to-date information is placed in the shared areas of the Web site. As Code 15 begins the rollout of this new capability, additional training material and information will be disseminated.

9. Guidance contained in this Gen Admin will be incorporated into a forthcoming version of NCIS-1, Chapter 27.

10. Questions or comments regarding the NCIS Web site governance policy should be directed to (b)(6) Code 15A, at (b)(6) @navy.mil or (b)(6)

DISTRIBUTION
NCISHQ: All Directorates and Departments
ACTION: FOXX/All Directorates

CHAPTER 29
TITLE: SPECIAL AGENT AFLOAT PROGRAM
POC: CODE 24
DATE: MAR 08

29-1. GENERAL

29-1.1. Historical Background. The Naval Criminal Investigative Service (NCIS) Special Agent Afloat (SAA) Program was initiated in Europe during March 1967. Since its inception, the purpose has been to provide professional investigative support to afloat operational elements of the Department of the Navy (DON) wherever they are located throughout the world. Previously, special agents served on various ships in response to specific requests for assistance during deployment. From the beginning, the program was a success, and, in April 1971, a special agent was assigned to a deployed carrier for a period of six months with the designation of SAA. Progress continued, and by 1978, SAA personnel were assigned to each operational aircraft carrier in the U. S. Navy for a one-year assignment. In 1986, two SAA personnel, one focusing on Law Enforcement/criminal investigations and one on Foreign Counterintelligence (FCI), were assigned to aircraft carriers in an effort to determine the feasibility and effectiveness of having two agents assigned full time while deployed. This was discontinued when no longer considered viable. All special agents are eligible to serve in the program and can be called upon at any time to fill manning requirements; however, there has been a sufficient quantity of qualified volunteers to fulfill program requirements in the recent past.

29-1.2. SAA Program. The SAA Program assignment is one of the most demanding, challenging, and visible assignments that a special agent can experience during their career. The performance of the SAA can have a long-term impact on the professional reputation of NCIS. The SAA is expected to be conversant with all operational aspects of the NCIS mission, with specific experience on preventing terrorist attacks against DON forces, protecting sensitive information and reducing criminal activity.

29-2. AGENT SELECTION AND ASSIGNMENT

29-2.1. The SAA Program is managed by the SAA Program Coordinator (Special Agent, GS-13), with prior SAA experience, assigned to the NCIS Headquarters (NCISHQ) Deployment Support Office (DSO), Code 24B. The duties of the program coordinator include, but are not restricted to: provide advice on SAA Program matters to NCIS Senior Leadership and other headquarter elements; be involved in the screening and selection of special agents for the SAA program; provide input for the NCISHQ SAA seminar; maintain seat of government contacts regarding the SAA Program; and, ensure that operational and logistical support for all SAA personnel is standardized and upgraded.

29-2.2. All aircraft carriers, when deployed, will be staffed with one SAA. When in a non-deployed status, an aircraft carrier will be staffed with a SAA; however, depending upon the carrier's in-port status, the special agent may or may not be designated as an SAA. Extended shipyard periods for an aircraft carrier may not require the services of a SAA. Coverage for the ship during these periods may be provided by personnel from the NCIS Resident Agency (NCISRA) which has responsibility for the shipyard or ship repair facility at which the aircraft carrier is temporarily located. Additionally, SAA's will be assigned to deploying Amphibious Squadrons (Expeditionary Strike Groups (ESG)) and to deploying Fleet Staffs in the capacity of Staff Counter-Intelligence Officer, as applicable.

29-2.3. The eligibility criteria for SAA assignment selection are:

a. A special agent must have a minimum of three years as a credentialed NCIS special agent (a combination of military and/or civilian credentialed time will be accepted), or, three years creditable service as a credentialed military investigator (USA CID/AFOSI/USMC CID), or, a civilian law enforcement officer under the special law enforcement retirement provisions. SAA candidates must meet these eligibility requirements prior to reporting to the SAA assignment.

b. A special agent at the GS-12 level, regardless of the time-in-grade when the afloat vacancy is announced, is eligible for SAA consideration. A special agent with one year or more time-in-grade as a GS-12, will be promoted to GS-13 upon assumption of SAA duty, provided the special agent also received a "fully acceptable" rating on the Performance Appraisal Review System (PARS) evaluation for the preceding 12 months. This eligibility also requires favorable endorsement by the special agent's current Special Agent in Charge (SAC). A GS-12 special agent with less than one year-in-grade at the time they report to the SAA assignment will be promoted when they have completed one full year-in-grade, provided they received a "fully acceptable" PARS rating for the preceding 12 month period and are favorably endorsed by their current Supervisory Special Agent (SSA) and SAC. (For agents serving in an SAA assignment at the time of their eligibility for promotion, their "current SSA and SAC" are the SSA and SAC with cognizance over the SAA assignment.) Special agents deemed ineligible for promotion to GS-13 during or after completion of their SAA assignment will be subject to current GS-13 promotion policy.

c. The following criteria must be met by ALL candidates vying for consideration of an SAA assignment:

(1) A candidate must be conversant in all aspects of the NCIS mission, which include

preventing terrorist attacks against DON forces, protecting sensitive information and reducing criminal activity on DON operations.

(2) A candidate must possess a demonstrated competency in all aspects of independent duty, to include administrative processes, briefings, investigations and operations.

d. The SAA, when deployed, represents NCIS independently, functioning with little or no direct access to guidance from the NCIS supervisory chain. As such, the SAA's tact, judgment, professional and supervisory capabilities must be of an unusually high degree. Only the most highly qualified special agents will be selected to serve in the SAA Program.

29-2.4. The current SAA assignment is for one year, but future program requirements and operational initiatives could establish new tour lengths. Until then, consideration will be given to requests for extensions based upon specific reasons such as completion of deployment, etc. Once accepted into the program, the SAA is required to serve a full one-year tour; however, the SAA could be released sooner depending on the needs of the program. Efforts will be made to select special agents approximately 6-12 months in advance of their assignment. This will allow the prospective SAA an opportunity to attend the SAA seminar and plan for the assignment well in advance of the reporting date.

29-2.5. Prior to the completion of the SAA tour, the SAA will have the choice of exercising a three year "no move" option (see section 29-10.13) or bidding for an advertised vacancy. To assure the SAA optimizes the opportunity to remain in place when exercising the "no move" option, coordination should be made with the operational control field office, Codes 10A and 24B. To ensure the availability of a local billet, this coordination should be accomplished a year prior to completion of the tour of duty. This will allow the control field office to convert the SAA to a vacant billet, or to be carried as a temporary acceptable overage until a vacancy arises. If the SAA chooses to relocate (Permanent Change of Station (PCS)) and bid on an advertised vacancy, he/she would receive due consideration for the chosen vacancy, taking into account the successful completion of their SAA assignment.

29-3.ORGANIZATION AND OPERATIONAL CONCEPT

29-3.1. The SAA Program requires long range projections, selections, and training of SAA candidates. The current policy of assigning only qualified GS-12 and GS-13 special agents to SAA billets is considered essential to support the enhanced investigative and counterintelligence initiatives envisioned for all current and future SAA personnel. In order to fulfill the NCIS requirements, the below policy guidance is pertinent.

29-3.2. SAA Candidate:

a. The special agent desirous of a future SAA assignment may submit the request to NCISHQ (jointly to Codes 10A and 24B) via their respective SAC.

b. The supervisor will monitor the special agent's potential and suitability for SAA duty, which should be documented in Performance Narratives (PNs).

c. The performance of the candidate will be tracked by the manager and must remain progressively satisfactory.

d. A candidate can volunteer to serve on a specific ship. SAA assignments will be staffed by volunteers so long as sufficient qualified candidates exist at the GS-12 and GS-13 levels. The lack of qualified volunteers will make it necessary for selection of special agents who may not have volunteered to satisfy the needs of the program.

29-4. OPERATIONAL CONTROL

29-4.1. A SAA NCISRU is permanently placed under the operational control (OPCON) of the field office with geographical responsibility for the homeport of the afloat vessel. The homeport field office shall support the SAA NCISRU in the same manner as it would any other NCISRU in the area of responsibility (AOR). The OPCON remains with the homeport field office even when the SAA NCISRU deploys. When a SAA NCISRU is deployed, the field office located in the area of forward deployment (referred to as the forward deployed field office) is responsible to provide support, control, and guidance to the SAA NCISRU. The following guidance is provided to outline duties/responsibilities of both the homeport and forward deployed field offices:

a. The homeport field office will provide to the forward deployed field office (Mediterranean - Europe Field Office/NCISRA Sigonella; Red Sea/Persian Gulf/Arabian Sea - Middle East Field Office, Bahrain; WESTPAC - Far East Field Office, Yokosuka) a summary of significant ongoing investigations and other significant SAA activities not later than the actual date of deployment.

b. If applicable, NCISHQ components will provide copies of all operational and administrative documentation pertaining to an SAA NCISRU to both the homeport and forward deployed field offices for information and to monitor investigative activity.

c. The homeport field office will continue to process and control all reporting documentation and provide administrative guidance and direction to the SAA with information copies to the forward deployed field office.

d. The forward deployed field office will provide operational guidance and direction via the appropriate method of communication consistent with the classification level of the subject matter. Personal visits will be made by the SAC, Assistant Special Agent in Charge (ASAC), or designated SSA of the forward deployed field office whenever feasible and as the ship's operational commitments dictate. Every effort will be made to visit the SAA NCISRU when operating in the AOR of the forward deployed field office. The SAA will also maintain contact with the forward deployed field office through interaction with cognizant special agent referents while operating in the region. The forward deployed field office will provide evaluation comments to be included in the preparation of the PN by the homeport field office. A copy of those evaluation comments will also be provided to the NCISHQ SAA Program Coordinator.

e. While under the oversight of the forward deployed field office, special attention will be given regarding matters of quality of investigative product, host command relationships, collection

operations, narcotics interdiction operations, and related maritime security matters. The forward deployed field office will ensure there is advance notification of port visits by the afloat vessel to permit coordination of the above matters and provide a post visit report containing items of interest such as liaison contacts, “Sources’, and significant counterintelligence, counterterrorism, investigative and legal matters.

f. The forward deployed field office will provide all logistical support possible for the SAA while in their AOR.

g. There should be a continuous flow of communication and coordination between the homeport and the deployed field offices during the deployment periods to achieve the highest quality of supervision. Close coordination between the homeport and forward deployed field offices will prevent the duplication of administrative and operational management and guidance to the SAA NCISRU.

29-5. COMMAND RELATIONSHIPS

29-5.1. The SAA will normally provide direct support to the aircraft carrier, or other vessel to which assigned, or will directly support a Battle Group Commander, Amphibious Squadron Commander, or Fleet Staff. The SAA assigned to a specific ship will be expected to keep the Commanding Officer/Amphibious Squadron Commander apprised of all pertinent developments. The SAA assigned to a Battle Group will apprise the Battle Group Commander (generally, via the Chief of Staff) while maintaining a close relationship with the Commanding Officer and Executive Officer of the host ship.

29-5.2. Aircraft carriers routinely have a number of civilians on board and they are generally afforded the courtesies and accommodations commensurate with comparable officer rank. The SAA is also afforded the equivalent military officer's rank and normally considered a member of the Commander's Staff. The SAA usually receives distribution (via "shotgun routing") of all ship and/or staff message traffic classified below Secret with access to higher classified traffic only on a need-to-know basis. The SAA is usually invited to attend staff and/or social functions. The receipt of such courtesies requires assumption of correspondent responsibilities on the part of the SAA. The SAA must be constantly vigilant to the needs of the Commanding Officer and/or Task Force commander. The SAA should keep the Commanding Officer, Executive Officer and Chief of Staff informed of investigations in progress, provide timely briefings on situations that have a bearing on the security or general interest of the Fleet, and be alert to other general matters of interest. Additional information pertaining to military/civilian pay grade equivalency and benefits can be found on the following link: http://www.history.navy.mil/library/online/comparison.html.

29-5.3. The SAA should always bear in mind that a mutual spirit of cooperation and courtesy between agent and the serviced command will make the afloat assignment as enjoyable as possible.

29-6.SHIPBOARD PROTOCOL

Life aboard an aircraft carrier or other large USN vessel may seem rather complex at first, particularly to those special agents who have not previously served aboard a Navy ship. The Navy is

tradition laden and an aircraft carrier is sufficiently large to permit the practice of many customs and courtesies. It is customary that you remove your hat (uncover) upon entering the Ship's Wardroom; there should be no conversation or movement about the ship during the evening prayer; arrival aboard and departure from the ship should be made from the forward (brow) gangway; one should come to a position of respect and face the flag (colors) located astern, and then request permission from the Officer of the Deck (OOD) before coming aboard. These are but a few of the many customs and courtesies each special agent should become acquainted with through applicable reading and orientation prior to reporting for duty as an SAA. Recommended reading is found in the Navy Officer's Guide, Chapters 4 and 5, available in any Navy library. **Appendix (1)** to this chapter provides a more detailed introduction to shipboard protocol.

29-7. COMMAND SUPPORT

29-7.1. Commander, U.S. Pacific Fleet Instruction 5402.1 (Series) and U. S. Fleet Forces Command (USFFC) Instruction 5300.3 (Series) set forth guidance to Commanders with regard to support of the SAA Program. The Commanding Officer of the carrier will have provided a private stateroom for the SAA and a suitable office space, which will include required storage for classified material and evidence. Effective and continued liaison with the command will assist in ensuring problems with the living and work spaces do not occur.

29-7.2. Administrative Support. Deployed aircraft carriers may have an assigned NCIS Yeoman to provide administrative support. Depending upon circumstances, an aircraft carrier located at a homeport field office may also have a NCIS Yeoman assigned aboard. Prospective NCIS Yeomen routinely undergo a modified background investigation to ensure their suitability for assignment to an NCIS component. NCISHQ maintains liaison with the Naval Personnel Command (NPC) regarding yeoman support.

29-7. 3. Photography and Reproduction. Photographic and reproduction services are generally available aboard larger Navy ships. It would be a rare instance when the SAA will not be able to obtain these services. There should also be no problem in obtaining an ample supply of required expendable supply items.

29-7. 4. Eating Arrangement. The SAA is paid a set per diem rate, which is sufficient to pay for daily meals in the Wardroom. Since procedures for belonging to the Officer's Mess vary slightly from ship to ship, it is recommended the SAA contact the Wardroom Mess Treasurer to make suitable arrangements.

29-7. 5. Personal Services. There are ample personal services available aboard ship, i.e., laundry service is free. Simple shipboard procedures are easy to learn. Although the disbursing office will normally cash personal checks, it is highly recommended the SAA obtain a personal internationally accepted credit card in addition to the U.S. government travel credit card. Also, it is recommended the SAA request the homeport field office assists to increase the credit limit on the government travel credit card to the maximum allowable amount. This will prove invaluable when going ashore in foreign or domestic ports, especially if faced with unplanned or emergent travel requirements. Other financial situations are discussed in the following sections.

29-8. OPERATIONAL PROCEDURES

29-8.1. Component Code Assignments. Each afloat NCISRU is assigned a permanent component code. There will be no change in the component code assigned unless a host ship changes homeport permanently, or is located at a stationary point (i.e., shipyard) outside the homeport field office's AOR for a prolonged period of time.

29-8.2. Case Control Numbers. The Case Control Number (CCN) used by the SAA NCISRU will be sequential for each initiated case (b)(6) (b)(6) The sequential CCN will be used by the SAA NCISRU while deployed, on local operations, or in any port, including the homeport. The sequential CCN will start over with '0001' on January 1, as is the practice in all NCISRA/RU offices. The SAA NCISRU submitting the document will be identified in the "MADE AT" entry. ESG SAA's and deployed Fleet Staff Counterintelligence Officer (SCIO) SAA's will utilize the CCN obtained from their respective homeport field offices.

29-8.3. File Retention. Upon completion/termination of the SAA assignment, the SAA may destroy those investigative notes no longer required for administrative/court martial action. However, where such action is contemplated and/or pending, rough notes should be forwarded to the homeport NCISRA for inclusion in the case file. The homeport NCISFO/RA need retain reports only for the mandated file retention period. (See NCIS-1 Chapter 25, Report Writing.)

29-8.4. Sources. When the afloat NCISRU deploys, the "Source" work folder should accompany and be maintained by the SAA. Source reporting must be performed in accordance with the procedures detailed in Manual NCIS-3 Chapter 8.

29-8.5. Distribution of Reports. The afloat NCISRU is authorized to make direct distribution to the homeport and forward a copy to the deployed field office. When a NCISHQ component transmits an investigative tasking to the afloat NCISRU, it will be sent by SSD as a ROI (LEAD) to the homeport field office, with an "INFO" copy to the forward deployed field office. The homeport field office will forward the lead via email to the afloat NCISRU. This procedure will allow the SAA to commence coverage of leads expeditiously. The SAA will address the results of the completed lead in the appropriate NCIS reporting format and forward the document as an email attachment to the homeport field office for distribution. The SAA is encouraged to provide brief, concise, reports in lead responses.

(b)(7)(E)

29-9. ADVANCE PARTY PARTICIPATION

29-9.1. During deployment, an aircraft carrier and accompanying ships routinely visit many ports in its area of deployment. Routinely, the ship will send an advance party to the port several days prior

to the port visit to take care of logistical matters for the entire carrier group. Usually, a representative from the ship's Supply Department, Senior Shore Patrol Officer, Beach Guard Officer, NCIS SAA, and, possibly, Legal Officer participate in advance party activities. It is extremely important that coordination of the port visit be made with the respective field office or NCISRA which has operational responsibilities over the prospective port to be visited and with the cognizant country referent. This coordination will allow for the NCIS component and referent to provide the best possible support in preparation to and during the port visit and ensure deconfliction with field office/NCISRA operational activities.

29-9.2. (b)(7)(E) (b)(7)(E) Again, it is extremely important that any operational activities in the port to be visited be coordinated with the cognizant field office and/or NCISRA. The NCIS Referent Program was established to maintain long term relationships with host country officials and provide the visiting USN/USMC components with up to date, accurate information relative to the port and the surrounding region. Meeting with the referent special agent during the advance enables the SAA to establish valuable points of contact and obtain the necessary elements of information required to provide a pertinent and timely port brief. The SAA should then be prepared to deliver a concise, detailed brief at the arrival conference normally scheduled a day or two prior to the arrival of the aircraft carrier/battle group in port. While in a port with little or no U.S. military presence, the SAA is encouraged to reside ashore at the applicable per diem rate where the SAA can collect information on a variety of matters (b)(7)(E) (b)(7)(E) (b)(7)(E) If warranted the SAA should be prepared to update port studies or to prepare port studies if none exist. Additionally, while living ashore, the SAA should make a serious effort to visit each ship in the carrier or battle group. Whenever the SAA resides ashore during a port call, the SAA should notify the Chief of Staff, Executive Officer, Shore Patrol Headquarters, and the Beach Guard of specific contact information regarding the hotel room, telephone number, and general itinerary, if at all possible.

29-9.3. Country Clearance. Prior to conducting any off-ship advance work, a country clearance request message must be submitted to the cognizant Department of State or Department of Defense (DoD) in-country or theater component. Each country has specific requirements and timelines. The DoD Foreign Clearance Guide (https://www.fcg.pentagon.mil/) provides guidance. Ensure that the servicing field office and NCISRA is courtesy copied on each country clearance message.

(b)(7)(E)

29-10. ADMINISTRATIVE AND FINANCIAL MATTERS

29-10.1. Pre-deployment Planning. A SAA aboard a deployed carrier occupies a very unique billet

in NCIS. The SAA is required to work independently for extended periods without benefit of direct supervision, guidance or assistance from their homeport field office. As a result, it is incumbent upon the agent selected for the SAA Program to formulate their plans and make all appropriate personal arrangements prior to deployment. The SAA must ensure that all personal affairs are in order, that they applied for and received all necessary documents, and that the onboard stateroom and office space are adequately stocked with all required supplies, equipment, forms and manuals. Further, each SAA must be thoroughly familiar with the operational and administrative aspects of an afloat NCISRU. A checklist containing numerous items of interest to the SAA is found in **Appendix (2)**.

29-10.2. The newly assigned SAA is encouraged to establish contact with the incumbent SAA aboard the ship as soon as possible. In responding, the current SAA should provide suggestions regarding wearing apparel, recommend personal comfort items and other information to assist their relief during the extended absence from home. Anticipated itinerary data should also be offered for required visa applications. All pertinent areas, including shipboard procedures, personalities, evidence storage (b)(7)(E) and ongoing investigations, will be discussed in detail with the new SAA.

29-10.3. Passports and Visas. The SAA should ensure that his/her passport is current and any required visas have been obtained. The SAA should obtain a no-fee authorization passport application from his/her field office. The requirement to submit country clearance request messages prior to conducting off-ship advance work is outlined in section 29-9.3 above.

29-10.4. Leave.

a. All timekeeping and leave records will be maintained by the homeport field office. The SAA will forward the time and leave data via email to the cognizant field office, where the applicable Standard Labor Data Collection and Distribution Application (SLDCADA) entries will be made. Should the SAA be temporarily assigned to the homeport field office, the SAA's parent field office will maintain the SLDCADA entries for the SAA. When leave is granted during deployment, the forward deployed field office assumes responsibility for the ship's investigative requirements in the absence of the SAA, and, if necessary, will designate a special agent from its office to relieve the SAA for a leave period or Temporary Duty (TDY). Whenever a SAA will be absent from the ship in a leave or TDY status, the SAA must ensure that command personnel know how to obtain investigative assistance, if required. If an interim/temporary SAA is assigned, they will assume the responsibilities of the primary SAA.

b. In addition to the regular accumulation of annual leave, the SAA accrues shore leave. Prior to deployment, while operating out of the homeport, one day of shore leave is earned for every 15 days spent at sea. Any consecutive seven-day period or more, at sea, is utilized to compute shore leave (this includes other ports of call). If not in a deployed status, any sea period of less than seven consecutive days does not apply toward shore leave. Further, once the actual deployment commences, one day of shore leave is accumulated every 15 days for the duration of the deployment regardless of whether the ship is at sea or in port. Shore leave must be used within six months after the agent is transferred to another NCIS component (non-SAA assignment), or, before the agent is separated from NCIS. As with annual leave, the homeport field office is responsible for computing

and maintaining a record of shore leave.

29-10.5. Stateroom, Equipment and Supplies. The homeport field office shall ensure that all homeport aircraft carriers, in their geographical AOR, provided appropriate stateroom accommodations for the SAA. The homeport field office is responsible for providing all directory/manual changes and pertinent NCIS administrative documents. The SAC or ASAC, or designated SSA of the homeport field office, will conduct an inventory (preferably in the presence of the SAA) of all equipment, supplies, manuals and forms during the SAA turnover and prior to all deployments.

29-10.6. Physical Examination. All special agents are required to have an annual or bi-annual physical examination. Unless the SAA assigned aboard the carrier will be under the control of the homeport field office and physically available when the physical examination is due, the SAA will make arrangements to obtain the examination aboard ship.

29-10.7. Travel. All special agents selected for the SAA Program are provided TDY orders issued by the field office to which the special agent is permanently assigned. These orders authorize multiple travel advances at 30-day intervals for incidental expenses aboard ship. Further, the TDY orders authorize additional amounts when the SAA is TDY off the ship where the per diem rate exceeds the daily shipboard rate. The broad scope of the orders allows for virtually all eventualities and requires the SAA to submit travel claims every 30 days. Whenever the SAA determines to be off the ship for more than 24 hours, the SAA should notify the homeport and forward deployed field office, providing a complete itinerary. Additionally, as a courtesy, the SAA should apprise the Commanding Officer or Executive Officer and/or the Commander or Chief of Staff of the Battlegroup of such departure and/or absence from the ship. Assistance in arranging for air transportation from the ship should be obtained through liaison with the Air Transportation Officer or Air Operations Officer.

29-10.8. Insurance. Commercial insurance companies frequently insert exclusionary clauses into policies to limit or exclude liability under certain unique conditions. The SAA should examine their policy, or, policies, for the existence of such clauses which might exclude payment of benefits for accident or death benefits while serving on a combatant in a theater of war, or, occurring aboard, "non-scheduled" or "military aircraft/vessels." Requisite riders to the policy may be obtained to cover these contingencies. The essential value of a current Last Will and Testament (LW&T) as a basic document in an orderly personal life should not be overlooked. The legal office aboard carriers will be able to prepare a LW&T if the SAA requests assistance.

29-10.9. Identification/Privilege Card. A special agent, designated for SAA duty, is authorized to obtain and use a Uniformed Services Identification and Privilege Card (DD Form 1173) Common Access Card during overseas status. Presentation of this card will allow the SAA access to the overseas military exchange, USO and other authorized overseas facilities. Additionally, it will entitle the SAA to special military rates or discounts at various overseas hotels. This card can only be utilized during the SAA's deployment overseas and must be surrendered or destroyed upon return to CONUS. Most ships can issue this card to the SAA. Otherwise, the card can also be obtained through the SAC of the forward deployed field office.

29-10.10. Firearms Aboard Ship. Under normal conditions, the SAA agent does not routinely carry a firearm while aboard a carrier or deployed vessel. Pertinent Navy instructions/regulations relating to firearms apply to the SAA's use and wearing of firearms aboard a Naval vessel. The SAA should either keep their firearm in their personal stateroom safe or in the ship's armory. Local conditions aboard ship may require the SAA to apprise the Commanding Officer and/or Executive Officer of the vessel to which the SAA is assigned that they have a firearm which is properly stored. The SAA must exercise extreme discretion in the wearing and use of a firearm aboard ship in accordance with requirements detailed in Manual NCIS-1 Chapter 34, Firearms, Use of Force, Intermediate Weapons and Ammunition. The SAA should also be aware that in many foreign countries, special agents are not routinely allowed to carry/wear firearms. The SAA should obtain current information from the forward deployed NCISRA.

29-10.11. Critique. Upon completion of a deployment/afloat assignment, the SAA is required to prepare a short, detailed, meaningful critique of the SAA tour of duty. The SAA will submit the critique to the SAA homeport field office coordinator and the DSO Code 24B. Pertinent information contained in these critiques will be furnished to applicable forward deployed field offices by NCISHQ. There is no established format for the critique, however, it should include comments regarding the logistical, administrative and operational support received from the afloat command, and both homeport and deployed field offices. The critique should be a concise, frank appraisal of the SAA Program, containing appropriate opinions, recommendations and conclusions. The SAA is encouraged to evaluate the conditions and procedures under which they operated, highlight existing and/or potential problem areas, and offer appropriate comments and suggestions to initiate meaningful modifications and improvements to the SAA Program.

29-10.12. Premium Pay. In order to meet the unique operational requirements of DON combatant ships to which an SAA is assigned, and to provide scheduling flexibility to fulfill the multifaceted operational needs of the NCIS mission, the following premium pay entitlements apply:

a. The SAA may have up to a maximum of 20 hours of Regularly Scheduled Overtime (RSO) scheduled during the administrative workweek (Sunday through Saturday). Any RSO required Monday through Friday must be scheduled after a ten (10) hour workday, which consists of the regularly scheduled 8 hours plus 2 additional hours, which, as dictated by legislation, is compensated as Law Enforcement Availability Pay (LEAP). Any additional hours that may be required beyond the 20 hours of RSO will be considered LEAP. Ten (10) hours of RSO can be scheduled on Saturday or Sunday. Thus, ten (10) weekend hours of RSO, combined with the up to ten (10) hours of RSO scheduled during the week, equals the 20 hours allowed per week. Work should be scheduled in advance of the scheduled workweek. RSO hours worked should be reported on the SAA’s time and attendance report.

b. The payment of RSO will continue to be allowed when the SAA’s assigned ship is in a port other than the homeport. Scheduled hours of overtime required while in ports other than the homeport will be compensated with RSO, as noted above. Although RSO may be scheduled in order to meet operational demands in other ports of call, the SAA is encouraged not to do so if special agents from the deployed AOR are available and providing support during the port visit. In such a circumstance, the SAA is encouraged to “take a break” if manpower and operational tempo permits.

c. Holiday Pay. A SAA performing non-overtime work during a regularly scheduled daily tour of duty on a holiday designated by federal law, or, executive order will be paid holiday pay. According to the Federal Personnel Manual (FPM), Chapter 550, holiday pay is equal to the hourly basic rate of pay for the actual number of hours worked on a holiday, not to exceed eight hours. For clarification, if a designated holiday occurs on a weekday while the ship is at sea, the SAA will receive eight hours holiday pay plus two hours RSO pay. If a designated holiday occurs on a weekday while the ship is in port, the SAA is not required to work a regularly scheduled daily tour of duty and any work performed during that day will be compensated as LEAP.

d. RSO hours worked must be completely documented. If the workload is not sufficient to justify RSO, the SAA will not otherwise be compensated for work not performed. Any other types of premium pay that may impact an SAA are contained in the Manual NCIS-1, Chapter 15, Hours of Work, Pay and Leave.

29-10.13. Additional SSA Benefits. Upon the successful completion of a SAA assignment the SAA will be entitled to a three year "no move" option, during which he/she may choose to remain at the field office where the SAA assignment originated. Coordination with the affected field office, Code 10A, and Code 24B will be required prior to selection of this option, as previously described in this chapter. The SAA may also choose to bid on advertised vacancies and will receive due consideration for these bids in respect to their successful SAA tour.

APPENDIX (1): INTRODUCTION TO SHIPBOARD PROTOCOL

1. CLOTHING AND PERSONAL EFFECTS

a. Clothing worn aboard ship should be comfortable, durable, and safe. Sturdy, comfortable shoes with non-skid soles are strongly recommended. The SAA can expect to do much walking, and climbing up and down ladders.

b. Dress slacks and casual shirts are appropriate for daily shipboard duties. Male SSA's should bring along a suit and/or sport coat and tie for dining in the wardroom on special occasions and during official functions while in port. Similar appropriate business attire for female SAA's is recommended. The SAA is responsible for acquiring their clothing.

2. WARDROOM ETIQUETTE

The SAA will join the officer's wardroom and normally dine in this facility. Dress for the evening meal varies with each ship, but is usually semi-formal. Breakfast and lunch are less formal, but the general rule of thumb is to be dressed equal to the officers present whenever possible. Blue jeans are never appropriate.

3. PRIVILEGES AND FACILITIES

A U.S. Navy aircraft carrier is completely self-contained with all of the necessary facilities normally found in a city with a population of 5,000 to 7,000. The ship's store will normally be open to the SAA.

4. GENERAL SAFETY PRECAUTIONS

Be alert to hazards during your stay. The combination of many high performance aircraft within the confines of a large vessel creates a situation that is potentially dangerous. Each person has a responsibility to themselves and their shipmates to use common sense and good judgment when it comes to safety. This section contains some general guidelines for your safety. It is also recommended the newly assigned SAA attend safety orientation when reporting aboard. General guidance is provided:

a. Fire. The hazard of fire aboard a carrier is always present. Should your compartment fill with smoke, the purest air will be on the deck (floor) since smoke and fumes are lighter than air and will begin collecting first along the ceiling. A wetted-down blanket will give protection against the heat and will act as a filter against smoke and fumes if placed over your head and shoulders. Be cautious when opening doors with bare hands; the metal will heat up quickly. If in doubt, push the door open with the sole of your shoe or some other object. Also be aware of potential high pressure being built up behind closed and/or sealed doors. If hard to open, use extreme caution when attempting to force the door as the pressure behind it could cause an explosion when opened.

b. Smoking Precautions. Smoking is not permitted on weather decks, flight decks, or hangar decks. During all emergency drills, whenever the ship is taking on or discharging fuel, and when

transferring any munitions or combustibles, smoking is forbidden throughout the ship. Before any operations begin, an announcement will be made over the ship's public address system identifying the type of operation about to take place, and that smoking is not allowed until such operation is completed.

c. Safety in and Around Aircraft. The following general safety precautions are recommended when in and around aircraft:

(1) Never approach or board an aircraft unless authorized to do so. Beware of all movable surfaces (propellers, arresting hooks, control surfaces, speed brakes, folding wings, etc.). Arresting hooks can be released even with no electrical or hydraulic power applied.

(2) Be aware of where you place your hands. Use only designated handholds, control levers, and access provisions. Never grasp exposed flight control cables, leading edges of propeller blades or leading edges of compressor rotor or stator blades. Be very careful in areas of extreme temperature not to touch things such as exhaust pipes, transmission lines, or electronic black boxes.

(3) If the quarters are equipped with variable volume loudspeakers, the sound level should be kept at such a level that emergency announcements are easily heard.

(4) Always wear shoes when away from your stateroom. During a fire, metal decks and ladders heated by flames can become impossible to walk on barefooted.

d. Safety Drills

(1) In order to ensure your own safety, you should affect liaison as soon as possible after reporting aboard with the Damage Control Office. This office will assign your appointed station for Fire drills, Man Overboard drills, and General Quarters drills.

(2) Alternative escape routes from the stateroom to other areas of the ship should be planned and tested. Prepare to crawl from the stateroom area to the nearest, safest method to an exit in case of fire.

(3) Two emergency breathing apparatus devices should be in each stateroom, and it is imperative to become familiar with this equipment and the proper utilization.

5. FLIGHT OPERATIONS

a. During flight quarters, the flight deck is especially dangerous. This deck (combined with the hangar deck, magazines, and shops) provides the operating facilities equal to a large airfield, focused into a relatively small area. Among the more common flight deck hazards present during flight operations are:

-Jet blast and propeller/rotor wash

-Jet intakes

-Rotating propellers, helo-blades and tail rotors

-High wind and blowing particles

-High noise levels (wear ear plugs!)

-Pitching and rolling deck

-Moving elevators and yellow equipment

b. Nearly all flight deck accidents occur as a result of carelessness on the part of the individual, or, as a result of an individual being in areas where they have no business. The most dangerous areas are:

-The vicinity of the arresting wires, barriers, and barricades.

-The area along the angle deck and around the arresting gear.

-The port and starboard side catwalks.

c. There is only a small amount of area left, and even that is subject to occasional accidents. You will notice safety posters throughout the ship, and you will hear the expression "look alive". This means to keep your eyes open if you want to stay alive. For example, a tractor driver towing a multi-million dollar aircraft has two things on his mind; the deck edge and the yellow shirted taxi director. He has no time to watch out for "pedestrians". There are two tractor speeds: "stop" and "go". The "go" at times is rather briskly executed. Again, just look alive.

d. On the flight deck there is a maze of moving colors. Each man has a specific function; some individuals will be wearing colored jerseys or sweaters, cloth helmets (some with integral radios for communication), and goggles. The colors represent the following:

White with red cross - medical department personnel

White - safety department personnel

Green with identifying black letter - catapult and arresting gear crews

Green with or without squadron numbers - squadron maintenance personnel and manufacturers representatives

Purple - fuel handlers

Red with black stripe - ordnance personnel

Red with black letters REP 8, 5 etc. - damage and crash control

Yellow - deck handling officers, catapult officer and aircraft directors

Blue - plane pushers and chockmen

Blue with white "T" - tractor driver

Brown - plane captains and squadron personnel

Silver metallic suit - hot suit man attached to damage and crash control

e. The one location aboard the carrier where all facts are known and available, as far as flight operations are concerned, is the ship's control tower (Pri-fly). Here, all activity is directed and the commands are given by the "air boss". The air boss answers only to the ship's Captain during flight quarters.

f. Catapults. All carriers have catapults on the forward deck and on the angle deck. The catapults are steam-operated and provide great thrust. During a "cat shot," the aircraft is held in position by a trail bar or a holdback release assembly, and is attached to the catapult shuttle by means of a bridle or tow bar. When everything is in place, the slack is taken up by applying a predetermined tension load at the shuttle. The aircraft's engines are then accelerated, the catapult officer signals launch, and the horizontal load at the shuttle is increased. At a given load, the holdback element releases and the shuttle pulls the aircraft down the catapult.

g. Recovery. A lens system of landing is used to guide the aircraft "down the slot" and ensure proper hook-to-ramp clearance at touchdown. This system, known as the "Fresnel" lens, operates like a searchlight and provides the pilot with a beam of light (the ball) that is visible only when he is on the correct glide path. The pilot must keep the ball centered in the mirror between two illuminated horizontal arms extending from the sides. Since different types of aircraft have different lengths and pilot height-to-ground clearances, the lens or mirror may be adjusted for the particular aircraft along the glide slope. The raising or lowering of the mirror or lens effectively changes the height at which the tailhook will clear the ramp and engage the arresting wires. While observing flight ops you will see four arresting wires on the flight deck which are used to catch an aircraft's tailhook. An aircraft perfectly landed will pick up the third in a series of four wires, counting from aft of the ship.

h. Night Operations. Night operations are doubly dangerous and it is recommended to stay off the flight deck at night unless escorted there. White light can be particularly hazardous on the deck at night. It can ruin someone's night vision for five to 10 minutes. Flashlights should be equipped with red lenses if used. Remember, any type of open flame is strictly prohibited outside of authorized smoking areas.

6. USEFUL TERMS AND ABBREVIATIONS

The Navy, like all other professions, has developed its own unique vocabulary. Some of these terms are as old as the Navy itself; others are as new as the latest technology. Additional information on

terms and abbreviations may be found in the Navy Officer's Guide or the Bluejacket Manual.

a. General terminology (in alphabetical order):

AIR BOSS - Air Officer; controls flight operations
BATTLE GROUP - An aircraft carrier and her escorts
BOW - The front part of the ship
BRIDGE - Located in the island from which the CO or OOD controls the ship
BULKHEAD - Wall
CAG - Commander Air Wing (pronounced kag)
CAT OFFICER - Catapult Officer
CDO - Command Duty Officer
CIC - Combat Information Center
CO - Commanding Officer
CPO - Chief Petty Officer
DECK – Floor
FIRST LT - (usually a CDR) Officer in charge of all deck operations other than flight deck
FLAG – Admiral
FLIGHT DECK - The large deck from which flight operations are conducted
GQ - General Quarters; call for battle stations to be manned
ISLAND - The large superstructure on the starboard side of the flight deck from which all operations are controlled
HANGAR DECK or HANGAR BAY - deck below the flight deck (aircraft are storage and maintenance)
HEAD – Toilet and/or Bathroom
JOOD - Junior Officer of the Deck; assistant to the OOD
KNOTS - Nautical miles per hour
LSO - Landing Signal Officer; controls landing operations
OFFICER'S COUNTRY - The general area around the wardroom and officer's staterooms
OOD - Officer of the Deck
OPS - Operations
PAO - Public Affairs Officer
PORT - Left; the left side of the ship
PRI-FLY - Located in the island in which the "Air Boss" controls flight operations
READY ROOM - Room assigned to each squadron for preflight briefings, etc.
STARBOARD - Right; the right side of the ship
WIRE - Arresting, used to land aircraft
XO - Executive Officer

b. AIRCRAFT/HELICOPTER TERMINOLOGY

AMCM - Airborne Mine Counter Measures
ASW - Anti-Submarine Warfare
BOLTER - Miss arresting wire when landing
COD - Carrier Onboard Delivery
GALLEY - Ship's kitchen

HELO/BIRD – Helicopter
HM - Helicopter Mine Counter-Measures
HS - ASW Helicopter Squadron
HSL - Helo ASW Squadron
'In the Groove' - A landing aircraft that is in the proper position on the glide path
LAMPS - Light Airborne Multi-Purpose System
PANTRY - Wardroom kitchen
SAR - Search and Rescue
VAQ – Electric Attack Squadron
VAW - Airborne Early Warning Squadron
VERTREP - Replenishment by helicopter
VFA – Strike Fighter Squadron
VMFA – Marine strike Fighter Squadron
VOD - Vertical Onboard Delivery
VS - ASW Squadron, Fixed Wing

APPENDIX (2): SPECIAL AGENT AFLOAT PROGRAM CHECKLIST EXTENDED PLANNING

- Review Manual NCIS-1 Chapter 29, Special Agent Afloat Program.
- Obtain Passport.
- Ensure Visas (if required) are obtained for intended countries to be visited.
- Obtain an international/universal acknowledged credit card.
- Ensure personal affairs are in order (i.e., LW&T, Power of Attorney for spouse, or other designated person, if required).
- Review Naval protocol, if needed.

FOUR TO SIX WEEKS PRIOR TO DEPLOYMENT

- If not already accomplished, effect liaison with CO, XO, Legal Officer Officer, Personnel Officer, CMAA, and the Disbursing officer.
- Insure necessary publications are available/accessible (NCIS-1, NCIS-3, (b)(7)(E) aboard ship (on CD or hard-copy).
- Conduct an inventory and obtain needed clerical and computer supplies, envelopes, stamps, forms, etc.
- Arrange for berthing and office space with respective ship personnel.
- Arrange for adequate classified material and evidence stowage.
- Inventory crime scene kit, photo equipment and film.
- Obtain Port briefs of areas to be visited from homeport field office.
- Purchase necessary clothing for afloat assignment, i.e., shoes, trousers, shirts.

TWO TO THREE WEEKS PRIOR TO DEPLOYMENT

(b)(7)(E)

- Inventory classified material on board.
- Inventory and purge evidence holdings in accordance with Manual NCIS-3
- Ascertain reporting station for general quarters and man overboard.
- Learn all available exits from your spaces in case of fire.
- Obtain your own EBD (Emergency Breathing device).
- Have sturdy flashlight available in the event of power failure.
- Learn procedures for laundry use, disbursing, etc.
- Set up official procedures for mail with ship's post office.
- Arrange for message release/pickup with ship.
- Instruct parent field office on any personal pay matters or other administrative requirements.
- Review shore leave accrual benefits.

(b)(7)(E)

ONE WEEK PRIOR TO DEPLOYMENT

- Arrange to join wardroom mess.
- Move additional gear aboard.
- Obtain any monetary advances on orders.
- Check with the Captain's office to ensure you are on the sailing list.
- Arrange for inoculations aboard ship (medical personnel aboard ship will be aware of requisite

shots for ports to be visited.

CHAPTER 30
TITLE: CREDENTIALS, BADGES AND PROTECTIVE SERVICE PINS
POC: CODE 11A
DATE: JAN 2010

30-1. INTRODUCTION

30-1.1. This chapter promulgates policy and procedures regarding Naval Criminal Investigative Service (NCIS) credentials, badges, and protective service pins. NCIS credentials are issued by the Director, NCIS to provide identification for civilian and military personnel authorized to represent NCIS in fulfilling the criminal investigative, counterintelligence, and security responsibilities of the Department of the Navy (DON).

30-1.2. Possession of credentials does not connote a security clearance; however, personnel issued "Special Agent" credentials are cleared for access up to and including Top Secret. In conjunction with credentials, four types of badges are issued: gold "Special Agent"; silver "Agent"; silver "Investigator"; and, silver "Operational Representative". The authority to carry firearms is reflected in the credentials and should not be tied to the issuance of a badge.

30-1.3. A set of four protective service pins (PSPs) is issued to authorized personnel to provide a unique visual recognition symbol between individuals assigned to a Protective Service Operation/Detail.

30-1.4. The Director, NCIS retains the right to withdraw or modify the credentials, badge, or protective service pins of any NCIS employee.

30-2. PURPOSE

To ensure proper issuance, control, and recovery of credentials, badges, and protective service pins in support of the NCIS mission.

30-3. TYPES OF CREDENTIALS

30-3.1. Special Agent. Issued only to 1811 Criminal Investigators and Marine Corps personnel designated as special agents. Where appropriate, the following titles can be included along with the designation of special agent in the blank title area: director, deputy director (DD), executive assistant director (EAD), assistant director (AD), deputy assistant director (DAD), and special agent in charge (SAC).

30-3.2. Agent. Issued to qualified and approved naval reservists who perform investigative or counterintelligence duties. Contact the NCIS Office of Military Support for additional information regarding the NCIS Reserve Program.

30-3.3. Investigator. Issued only to 1810 Investigators who perform investigative and/or counterintelligence duties.

30-3.4. Operational Representative. Issued to those NCIS personnel actively involved in operational aspects of criminal investigations and operations, counterintelligence investigations and operations, collection activity and analysis, and DON law enforcement and security. Employees who qualify for these credentials include, but are not limited to the following series: intelligence specialist/intelligence operations specialist (0132), investigations specialist (1801), foreign national investigator (FN pay grades), investigative computer specialist (2210), Physical security specialist (0080), training specialist (1712), forensic scientist (1301), evidence custodian (0303), and Department of Defense (DoD) military security personnel assigned/under the operational control of the NCIS Protective Operations Department, Code 21B.

30-3.5. Administrative Representative. Issued to NCIS professional administrative staff to conduct official business in furtherance of the responsibilities and mission of the NCIS.

30-3.6. All non-agent personnel authorized to carry a firearm in accordance with NCIS-1, Chapter 34 must be issued “Operational” or “Investigator” credentials with the appropriate lower credential, reflecting the employee’s authority to carry firearms while in performance of their official duties. These credentials will be issued on a limited basis with the approval of DAD, Security and Facilities Department (Code 11A) or his designee. Non-agent personnel authorized to carry a firearm on an occasional basis may instead be issued a standard lower credential and the OPNAV Form 5512/2 when required to be armed.

30-4. LOCAL CREDENTIALS

30-4.1. The field office SAC can authorize the issuance of a temporary credential card to personnel on a limited basis. Code 11A will issue a block of blank temporary credentials cards to each field office SAC. Temporary credentials shall not be issued for periods of more than one

year and must list the expiration date on the front of the card. This type of credential must be immediately withdrawn when the bearer leaves the direct supervision of the issuing field office element or when permanent credentials are issued. It will be incumbent upon the issuing authority to ensure proper control of the credentials and to recover them as soon as the immediate need has ceased. Temporary credentials may be issued to personnel in the following categories:

a. Newly hired special agent personnel until permanent credentials are issued.

b. Naval reserve personnel on active duty for training when it is desirable that they receive practical investigative experience.

c. Personnel assigned overseas. Some overseas NCIS offices have found it beneficial to provide personnel with a translation of permanent credentials in the language of the host country. This practice is left to the judgment of the SAC in consultation with the DAD, Code 11A. No specific requirements are established; however, these credentials must be of such quality as to uphold the professional image of NCIS.

30-5. DESCRIPTION OF CREDENTIALS

30-5.1 Permanent NCIS credentials consist of two cards that are completed, authenticated, and laminated. Card A (upper credential) identifies the agency, name, seal, and bearer title. Card B (lower credential) consists of a statement of authority, bearer photograph, credential number, and bearer signature.

a. Special Agent Card A is a white card with blue micro text and the letters “NCIS” in bold gray. The NCIS special agent seal (in gold) is located at the top left of the card, and the DON seal (in gold) is located on the top right of the card. The words “United States of America” are located on the top center of the card, and the words “Naval Criminal Investigative Service” are located on the bottom center of the card. The bearer’s name is inserted between the lines “This is to certify that” and “whose signature and photograph appear below is a duly sworn”, with the special agent credential title located underneath. The complete written title of Director, NCIS, and respective DD, EAD, AD, SAC, or DAD may be included when appropriate.

b. Special Agent Card B is a white card with blue micro text. The card includes the bearer’s photograph, credential number, date of issue, and a recitation of his/her authority. The bearer’s authority is outlined on the Director’s credential “by order of: The Secretary of the Navy”. The bearer’s authority is outlined on all other special agent credentials as: “is authorized as a Federal Law Enforcement Officer to carry firearms and conduct investigations of violations of the laws of the United States of America for the Department of the Navy.” The card is signed by both the Director, NCIS and the bearer. Special agent credentials will be issued in a black leather folded case with the NCIS gold “Special Agent” badge.

c. Agent Card A is a white card with blue micro text and the letters “NCIS” in bold gray. The NCIS seal (in gold) is located at the top left of the card, and the DON seal (in gold) is located on the top right of the card. The words “United States of America” are located on the top center of

the card, and the words “Naval Criminal Investigative Service” are located on the bottom center of the card. The bearer’s name is inserted between the lines “This is to certify that” and “whose signature and photograph appear below is a duly sworn”, with the agent credential title located underneath.

d. Agent Card B is a white card with blue micro text. The card includes the bearer’s photograph, credential number, date of issue, and a recitation of his/her authority. The bearer’s authority is outlined on all agent credentials as: “is authorized to carry firearms and conduct investigations of violations of the laws of the United States of America for the Department of the Navy”. The card is signed by both the Director and the bearer. Agent credentials will be issued in a black leather folded case with the NCIS silver “Agent” badge.

e. Investigator or Operational Representative Card A is a white card with blue micro text and the letters “NCIS” in bold gray. The NCIS seal (in gold) is located at the top left of the card, and the DON seal (in gold) is located on the top right of the card. The words “United States of America” are located on the top center of the card, and the words “Naval Criminal Investigative Service” are located on the bottom center of the card. The bearer’s name is inserted between the lines “This is to certify that” and “whose signature and photograph appear below is a duly appointed”, with the credential title “Investigator” or “Operational representative”, as appropriate, located underneath.

f. Investigator or Operational Representative Card B is a white card with blue micro text. The card includes the bearer’s photograph, credential number, date of issue, and the recitation of his/her authority. A variation of this lower card, which adds the authority to carry a firearm while in performance of official duties, will be issued to those personnel who have been authorized to carry a weapon. The card is signed by both the Director and the bearer. Investigator or Operational Representative credentials will be issued in a black leather folded case with the NCIS emblem or, if authorized, the appropriate NCIS silver badge.

g. Temporary credentials. The temporary credential is a single blue card and contains the DON seal. The bearer’s title (i.e., special agent) is typed in the space below “Naval Criminal Investigative Service.” The bearers name is typed below the words, “whose picture and signature appears hereon is.” The bearer’s photograph, the embossed NCIS seal, and a recitation of the authority title are typed on the card. The credential number and the expiration date, which should not be for more than one year, appear at the bottom of the card, followed by the SAC’s signature and the bearer’s signature in black ink. Temporary credentials will be issued in the single window black leather folded case.

30-6. REQUESTS FOR PERMANENT CREDENTIALS

30-6.1. The DAD, Code 11A, will process requests for all permanent credentials, issue all permanent credentials, recover all permanent credentials and ensure associated COMPASS entries are effected on a timely basis. Requests for Special Agent credentials shall be submitted to Code 11A utilizing the current NCIS Form 5512/8 (Request for Permanent Credentials) found in the Administrative Forms section on the NCISnet and shall include a digital photograph of the employee for whom the credentials are requested and a signed signature card. The NCIS special

agent coordinator (Code 10B) shall initiate requests for permanent credentials for personnel attending the Special Agent's Basic Training Program (SABTP) at the Federal Law Enforcement Training Center (FLETC), Glynco, Georgia. All other requests for permanent credentials will be initiated and approved by the SAC, appropriate DAD, or Director, NCIS. The NCIS security manager must review and approve all requests for permanent credentials. No credential request (non-1811) may be submitted to Code 11A without a security clearance. A Top Secret security clearance is required for special agent credentials. Final authorization from DAD Code 11A must be obtained before credentials will be issued.

30-6.2. Photographs judged not to be of suitable quality will be returned to the requester. All photos must be taken with a digital camera with the following requirements:

a. The background for the photo must be light blue and wrinkle/crease free.

b. The required photo image size measures 1.13 inch wide by 1.34 inch high. The individual should be centered with the distance from the top of the head to the chest measuring 1.25 inches.

c. Individuals must be dressed in business attire.

d. The photo must be submitted on a CD. Rename the file to the subject's last name, followed by a period, the initial of the first name, a period after the initial, and the file extension .jpg (example: Doe.J.jpg). If you do not include the file extension ".jpg", the image will not be retrievable. Submit only one image per individual, deleting images that will not be used. Attach a list of each individual by name in the order they appear on the disk or CD.

e. The signature card must be submitted with the signature of the individual requesting credentials. The signature card may be printed from the Human Resource Directorate (Code 10) website. Field offices must provide a hard copy of the signature card to subordinate offices that have no access to the website. Print the block for signature on heavy paper. The following are the guidelines listed on the signature card and other instructions:

(1) The signature card must contain the printed name and signature of the requestor; and,

(2) The individual signature must be contained within the designated box and shall not extend outside the lines; and,

(3) The writing instrument must be a black fine to medium point marker, heat and water resistant, smear-proof and permanent ink.

(4) Forward the CD containing the images along with the signature cards to Code 11A via FEDEX.

30-6.3. Permanent credentials for special agent personnel will be issued upon graduation from the SABTP at FLETC provided the individual has been authorized interim access to Top Secret information following a satisfactory National Agency Check (NAC) and submission of all required Single Scope Background Investigation (SSBI) paperwork submitted. Permanent

credentials will not be issued until security clearance requirements have been met. All other permanent credentials will be sent via registered mail to the field office concerned or delivered to and signed for by the bearers at Code11A.

30-7. REISSUE OF PERMANENT CREDENTIALS

30-7.1. Permanent credentials bear no expiration date. Credentials will be re-issued where appropriate when the credentials are lost or stolen, the bearer legally changes his/her name, the bearer's title changes, the condition of the credential is not acceptable, or the photograph no longer portrays a reasonable likeness of the bearer. The growth of a mustache, or other substantive change in appearance, is considered sufficient reason for requesting new credentials, provided the credential holder has demonstrated that such a change to their appearance is not temporary. It is the responsibility of the field office to ensure that credential photographs portray a reasonable likeness of the bearer and are presentable from an appearance point of view. Requests to reissue credentials will be initiated by the individual on the current NCIS Form 5512/8 and forwarded to Code 11A via the chain of command.

30-7.2. Replacement for worn credential cases may be obtained by submitting a written request to Code 11A.

30-8. BADGES

30-8.1. A gold colored NCIS badge, inscribed with the words “Special Agent” will be issued only to special agents upon graduation from the SABTP. Special agents possess police powers, i.e., they can arrest (civilian special agents only), apprehend, seek and execute warrants, search and seize property, and perform other tasks identified as the exercise of police powers. NCIS special agent badges are issued for the duration of a special agent's career, or in the case of U.S. Marine Corps personnel, the length of assignment as a Marine special agent (MSA). MSAs will also receive a gold colored NCIS badge inscribed with the words “Special Agent” upon successful completion of an NCIS initiated background investigation and commencement of their assignment to NCIS, if they are not immediately able to attend the SABTP.

30-8.2. A gold colored NCIS badge, inscribed with the words, “Special Agent” will be issued to newly hired 1811s upon commencement of their assignment to NCIS, if they served as 1811s with another federal agency immediately prior to their employment with NCIS and if they are not immediately able to attend the SABTP.

30-8.3. A silver colored NCIS badge, inscribed with the word “Agent”, will be issued only to personnel assigned to NCIS Navy reserve units once they have been accredited by Director, NCIS to perform investigative duties, and to newly hired 1811 criminal investigators, other than as provided in 30-8.2 above, who are not immediately able to attend the Criminal Investigator Training Program.

30-8.4. A silver colored NCIS badge, inscribed with the word “Investigator” will be issued to Investigators (1810).

30-8.5 A silver colored NCIS badge, inscribed with the words "Operational Representative" will be issued, when authorized in accordance with section 30-9, to personnel who participate as non-law enforcement officers in the operational aspects of criminal and counterintelligence investigations and operations, collection activity and analysis or DON law enforcement and security. Silver "Operational Representative" badges do not authorize the exercise of police powers.

30-8.6. The DAD Code 11A is responsible for issuing badges and ensuring information is entered into COMPASS as appropriate. No other badges are authorized except as provided in this chapter. Any duplication of an NCIS badge is unauthorized and may be a violation of 18 U.S.C. 701 and 716.

30-9. ISSUANCE OF NON-POLICE BADGES

30-9.1. The Director may authorize an NCIS employee to carry the "Operational Representative" non police silver badge in circumstances that meet the following criteria:

a. The employee is participating as a non-law enforcement officer in the operational aspects of criminal investigations and operations, counterintelligence investigations and operations, collection activity and analysis or DON law enforcement and security, including protective security operations; and

b. The employee is performing duties that require interaction with the public or other law enforcement personnel under circumstances in which immediate recognition of a law enforcement affiliation is required to ensure the employee's safety or to effectively accomplish his/her assigned operational duties.

30-9.2. "Operational Representative" badges issued pursuant to this authorization are non-police badges that accurately reflect the employees' operational duties. They confer no police powers including, but not limited to, authority to arrest, apprehend, seek and execute warrants, search and seize property, enter without permission or carry a firearm. They specifically do not authorize the bearer to violate traffic or other laws. Use of a non-police badge issued pursuant to this chapter for any purpose other than to identify the employee's law enforcement affiliation and official purpose is not authorized. Use of a non-police badge to state, imply or exercise police powers or other rights, privileges or access reserved to special agents or other law enforcement officials is serious misconduct that may result in disciplinary action up to and including removal from federal service and may be a criminal offense.

30-9.3. Authorization to carry a non-police badge is contingent upon consideration of all relative circumstances and must be in connection with the employee's professional responsibilities, accomplished within all relative guidelines set forth below, and authorized as the exception rather than the rule, after careful scrutiny of the situation effecting this authorization by the Director, NCIS.

30-9.4. Non-agent personnel will only be issued Operational Representative badges after the following process is complete. Respective SACs or DADs must submit written justification of

the request for non-police badge by employee name to their respective AD or EAD, who will coordinate all requests with the NCIS Inspector General (IG), Code 00I, for concurrence. If the requirement is of a continuous nature, written authorization must be revalidated each calendar year. If the requirement is temporary, such as for a particular investigation or operation, the authority is limited to the duration of the requirement as set forth in the request.

30-9.5. The initial burden and responsibility for this authority rests with the SAC/DAD, and ultimate approval authority rests with the DAD Code 11A along with IG concurrence. In almost all cases, official credentials are sufficient to identify the employee as a NCIS official representative. It is therefore incumbent upon the SAC/DAD to carefully scrutinize these requests to determine whether there is an actual and exceptional need for immediate recognition of law enforcement affiliation to allow the employee to safely and effectively perform his/her assigned duties.

30-9.6. All non-agent personnel who are authorized to carry Investigator, or Operational Representative badges will carry corresponding credentials issued by Code 11A. Authority for all non-agent personnel to carry a badge is limited to being in the actual performance of official duties. Weekends, after-hours when not on duty, and leave periods are examples of times when authority for such personnel is not applied.

30-9.7. Discontinuation of Authorization. NCIS EADs, ADs, DADs, and SACs are authorized and required to recover Investigator and Operational Representative badges from NCIS personnel when the badge is no longer required or, in their judgment, such retrieval is in the best interest of the service. A verbal report of this recovery shall be made to NCISHQ Codes 11A and 00I immediately, or as soon as possible, and written notification within two working days. The badge shall be returned to Code 11A by registered mail along with the written notification.

30-10. CARRYING OF CREDENTIALS AND BADGES

The credentials and badges issued to NCIS personnel shall be carried during all periods of duty unless operational circumstances dictate otherwise.

30-11. USE AND PROTECTION OF CREDENTIALS, BADGES, AND PROTECTIVE SERVICE PINS

30-11.1. Badges and credentials are issued to authorized personnel as a means of identification to conduct official government business. Duplication of these controlled items is unauthorized (18 U.S.C 701). Use of these items for purposes not directly related to official business is strictly prohibited and shall be cause for legal or disciplinary action (18 U.S.C. 701 and 716).

30-11.2. Personnel authorized to carry badges and credentials must not allow them to be removed from their control. However, when displayed for official purposes they can be examined as closely as is necessary to verify the identification of the organization and the scope of the bearer's authority. Such examination, however, must take place in the bearer's presence. A secretary will frequently attempt to use the credential as a calling card in announcing the bearer to their supervisor. Credentialed personnel should be alert to this and similar possibilities,

which would effectively remove credentials from the bearer's control. Tactful and courteous firmness will generally prevent potential embarrassment.

30-11.3. The protection of the badge and credential is the sole responsibility of the person to whom they are issued. The safeguarding of these items is vital and each holder must be aware of the serious repercussions which might result from their loss or compromise. It is impossible to identify the myriad of situations that might impact on the protection of badges and credentials. Attentiveness, good judgment and common sense are the guidelines to follow.

30-11.4. Generally, it is best to carry the badge and credential case as close to the body as possible so that absence can be easily detected. Carrying credentials in the breast pocket of a suit coat is not recommended as a general practice since the coat may be removed and be out of the direct control of the credential holder.

30-12. SECONDARY BADGES

The secondary badge is a second badge issued only to special agents, agents and non-agent personnel, who are authorized to be armed and are authorized to carry a gold or silver badge. These badges are to be used on a badge clip holder and attached to a belt on the waist. The carrying of the secondary badge is optional. The DAD Code 11A is responsible for issuing badges and ensuring information is entered into COMPASS as appropriate.

30-13. ACCOUNTABILITY

30-13.1. Code 11A is charged with maintaining accountability of all permanent credentials, badges, and protective service pins within the NCIS inventory. Additionally, Code 11A is responsible for maintaining within COMPASS an up-to-date inventory of all permanent credentials, badges and protective service pins issued to active NCIS personnel. Personnel authorized to carry permanent credentials, badges, and protective service pins shall retain them upon transfer to a new duty station within NCIS, except for personnel authorized to carry badges under section 30-9, who shall relinquish them upon transfer.

30-13.2. Inventory

a. There is no requirement to conduct an inventory at specific-timed intervals; however, credentials, badges, and protective service pins may be checked in the course of inspections and visits to subordinate components.

b. Badges, credentials and protective service pins authorized to be carried by non-agent personnel on only an occasional basis are to be controlled in the same manner as weapons. That is, a custodian must be appointed to maintain custody of the items, which will be checked out by the custodian at the beginning of a shift and checked in to the custodian at the conclusion of a shift.

c. Field offices must maintain a strict accounting for the issuance of temporary credentials. Numbers on the issued cards should be uniquely identifiable to the field office. The first two

digits are the first two letters of the field office code (example: Use "CA" for Carolinas Field Office), followed by a number running sequentially from "01" (example: CA01). Numbers assigned to local credentials are not to be reissued and a record of assignment, by number and bearer, must be retained for 5 years.

30-14. LOSS OF CREDENTIALS AND BADGES

30-14.1. In the event the credentials and/or badge (permanent or local) are lost, or for any reason cannot be recovered from personnel who have terminated their employment, an immediate report shall be provided to Codes 11A and 00I. Furthermore, a NCIS Category 2B investigation may be initiated by Code 00I in order to determine and document all circumstances surrounding the loss. This investigation shall be opened under the name of the bearer and shall be conducted by Code 00I or a designated supervisor.

30-14.2. Upon receipt of a report of the loss of a NCIS credential or badge, Code 00I will immediately effect an NCIC entry to advise other appropriate law enforcement agencies at the national level of the credential or badge loss. The responsible field office or NCIS Resident Agency shall undertake the notification of appropriate local, state and federal agencies.

30-14.3. If the lost credential is not recovered within 24 hours, the bearer should be issued local credentials. If the permanent credentials are not recovered within 15 days, a request for the new permanent credentials should be submitted using the current NCIS Form 5512/8. The justification block of the request should indicate "loss". The DAD for Code11A, after a thorough review of the circumstances of the loss, shall determine if the issuance of new permanent credentials is justified. If the new credentials are issued, they will bear a number different from that of the lost credential. If the lost credentials are recovered later, they must be forwarded to Code 11A for destruction. That credential number will not be reissued.

30-14.4. In the case of a lost badge, the DAD for Code 11A, upon notification from the concerned NCIS field office or department, may issue a replacement from inventory. The reporting and investigative requirements shall be the same as for a lost credential and NCISHQ shall determine the nature of any disciplinary action. If the lost badge is recovered after a replacement badge is issued, the employee may decide which badge to retain and the other badge will be forwarded to the DAD for Code 11A. In all cases involving a change in badge or credential number, an appropriate entry must be made in COMPASS by Code 11A personnel.

30-14.5. The loss of a locally issued credential must be reported and investigated in the same manner as a permanent credential. In the case of local credential, however, the issuing authority, field office, must determine if the circumstances of the loss justify the issuance of a new local credential.

30-15. RECOVERY AND DISPOSITION

30-15.1. All SAC, DAD and subordinate supervisors shall exercise particular care to ensure the recovery of credentials, badges and protective service pins from personnel who no longer require

them. Credentials, badges and protective service pins may not be retained as mementos other than as specified in section 30-16.

30-15.2. Disposition of credentials, badges, protective service pins and cases shall be as follows:

a. Permanent Credentials - Return to Code 11A by registered mail.

b. Badges - Return to Code 11A by registered mail.

c. Local Credentials - Local destruction by field office authorized.

d. Credential Cases - Local destruction authorized when no longer suitable for use.

e. Protective Service Pins - Return to Code 11A by registered mail.

30-15.3. The field office must report any recovery of permanent credentials, badges, or protective service pins immediately to Code 11A, who will update the COMPASS database.

30-16. RETIREMENT OF CREDENTIALS AND BADGES

30-16.1. Shadow boxes. Civilian and military special agents who retire from NCIS service and other NCIS personnel, who retire after completing 10 years of service with NCIS immediately prior to retirement, may elect to receive their credentials and, if applicable, their badges in an encasement known as a shadowbox.

a. Shadow boxes for special agents. Upon the retirement of a civilian or military special agent from NCIS service, the retiree may receive his or her credentials, badge(s) and protective service pins in an encasement called a shadow box. The responsibility for assembling and presenting a shadow box to a retiring special agent belongs to the agent's respective field office or NCISHQ department. In preparation for assembling the shadow box, the retiring agent's credentials should be submitted to Code 11A at least three weeks prior to the retirement ceremony. Code 11A will stamp the credential "Retired" and make the appropriate entries in COMPASS to reflect the status of the credentials, badge(s), and protective service pins. All credentials and badges issued during the retiree's career will then be sent back to the field office or NCISHQ department within fourteen days of receipt by Code 11A. The field office or NCISHQ department will then place these items into a shadow box and present them to the retiring agent. The credentials, badges and protective service pins are mementos within the shadow box and are not to be removed and carried. The funds for encasement must come from the employee or by voluntary donation in compliance with DoD ethics regulations and guidance; government funds may not be used. Any exception to this policy must have written approval from the DAD Code 11A.

b. Shadow boxes for other NCIS personnel. Any civilian employee or military member currently employed by or assigned to NCIS, who has been authorized to carry credentials, badge(s) and/or protective service pins, and who has completed 10 years of distinguished service with NCIS immediately prior to retirement, may receive his or her credentials, badge(s) and/or

protective service pins in an encasement called a shadowbox upon retirement. The responsibility for assembling and presenting a shadow box to a departing employee or military member belongs to the individual's respective field office or NCISHQ department. In preparation for assembling the shadow box, credentials should be submitted to Code 11A at least three weeks prior to the individual's departure. Code 11A will stamp the credentials "Retired" and make the appropriate entries in COMPASS to reflect the status of the credentials and badge(s), and protective service pins. The credential(s) will then be sent back to the field office or NCISHQ department within fourteen days of receipt by Code 11A. The field office or NCISHQ department will then place these credentials into the shadow box and present them to the departing individual. The credentials, badges and protective service pins are mementos within the shadow box and are not to be removed and carried. The funds for encasement must come from the employee or by voluntary donation in compliance with DoD ethics regulation and guidance; government funds may not be used. Any exception to this policy must have written approval from the DAD Code 11A.

30-17. RETIRED SPECIAL AGENT CREDENTIALS AND BADGE

30-17.1. Retired credentials. Special agents retired or retiring from NCIS may elect to receive retired credentials and badges. With respect to retired credentials, special agents will have the option of receiving a "Standard" single-card retired credential, or of receiving a two-card, retired credential that the agent may use in conjunction with a current state firearms certification in order to carry a concealed weapon during retirement in accordance with the Law Enforcement Officers Safety Act of 2004.

a. Law Enforcement Officers Safety Act of 2004. In accordance with 18 U.S.C. 926C, notwithstanding any other provision of the law of any state, or any political subdivision thereof, retired special agents of NCIS who meet the criteria of a "qualified retired law enforcement officer" may carry a concealed firearm that has been shipped or transported in interstate or foreign commerce so long as the qualified retired special agent is carrying appropriate photographic identification issued by NCIS (the two-card retired credential) along with a current firearms qualification certification (within the most recent 12 months) from the individual's state of residence. Additional information on these requirements may be found in DoD Instruction 5525.12.

b. Qualifications for receiving a two-card retired credential. Special agents retiring and currently retired from NCIS must meet the following qualifications in order to receive the two-card retired credential:

(1) Retired in good standing, other than for reasons of mental instability, as a law enforcement officer from NCIS; upon such retirement, and for an aggregate of 15 years or more, was authorized by law to engage in or supervise the prevention, detection, investigation, or prosecution of, or the incarceration of any person for any violation of law; and meets the remaining requirements listed below; or,

(2) Retired, after completing the initial probationary period with NCIS, due to service-connected disability as determined by NCIS; during service with NCIS, was designated by law to

engage in or supervise the prevention, detection, investigation, or prosecution of, or the incarceration of any person for any violation of law; and meets the remaining requirements listed below;

(a) Upon retirement had statutory powers of arrest. Of note, "statutory powers of arrest" has been interpreted by DoD as the power to arrest granted to civilian NCIS special agents under 10 U.S.C. 7480 and no other authority.

(b) Has non-forfeitable rights to benefits under the retirement plan of NCIS;

(c) During the 12-month period prior to the date of issuance of the two-card retired credential, the individual met, at his or her expense, the standards for training and qualification to carry firearms for active law enforcement officers in the state in which the individual resides;

(d) Is not prohibited by Federal law from receiving a firearm; and,

(e) Agrees not to carry a firearm pursuant to this policy while under the influence of alcohol or another intoxicating or hallucinatory drug or substance.

c. Description of two-card retired credentials. The NCIS two-card retired credentials consist of two cards that are completed, authenticated, and laminated. Card A (upper credential) identifies the agency, agency seal, name of bearer, and bearer title. Card B (lower credential) consists of a statement of authority, bearer photograph, credential issue number, bearer signature, and signature of the Director, NCIS.

(1) Card A is a blue-textured card with the letters "NCIS" centered in bold on the card's background. The NCIS seal (in gold) is located on the card's upper left corner and the DON seal (in gold) is located on the card's upper right corner. The words "United States of America" are centered between the two seals. The bearer's name is inserted between the lines "This is to certify that" and "whose signature and photograph appear below is a". The words "Qualified Retired Federal Law Enforcement Officer" in red lettering is located underneath. At the bottom of the card are the words: "Retired in good standing from the Naval Criminal Investigative Service as a Law Enforcement Officer on (date)."

(2) Card B is a blue-textured card with the NCIS seal (in gold) located on the card's upper left corner. A current photograph of the qualified retired law enforcement officer will be placed along the card's right edge with a credential number under the photograph. Next to the photograph will be the following statement:

"This card identifies the individual as a Qualified Retired Law Enforcement Officer in accordance with the criteria established in 18 U.S.C. 926C. In order for the individual to carry a concealed weapon, this card must be accompanied by a current firearms qualification certification (within the most recent 12 months) from the individual's state of residence. This card does not grant the bearer any authority to act on the agency's behalf or to exercise any law enforcement authority."

The lower card will be dated and signed by the qualified retired law enforcement officer and the Director, NCIS. Instructions for returning the credentials to Code 11A in case of loss by the bearer are on the back of cards A and B, as well as the email and phone number for the NCIS Multiple Threat Alert Center Watch.

d. Procedures for receiving the two-card retired credentials. Retiring or retired special agents who plan on carrying a concealed firearm in accordance with 18 U.S.C. 926C, must complete the following procedures in order to receive the two-card retired credentials:

(1) Retiring or retired special agents who meet the criteria for a "qualified retired law enforcement officer" outlined in section 30-16, must submit a written request to Code 11A for the two-card retired credentials.

(2) Any previously retired special agent who meets the criteria for a "qualified retired law enforcement officer" outlined in section 30-16, must submit a notarized statement to Code 11A attesting that he or she met the requirements contained in section 30-16 at the time of his or her retirement and that he or she is not now prohibited from carrying a firearm.

(3) The individual must also submit a current photograph and signature block (if not already present in the Code 11A credential database) in accordance with the procedures outlined in section 30-6.2.

(4) Prior to issuing two-card retired credentials, the NCIS Security Office must conduct a NAC on any individuals without a current, completed background investigation in order to establish that the individual is not prohibited from carrying a firearm.

(5) Prior to receiving the two-card retired credential, the individual must sign and return agreement of policy provided by Code 11A. Active special agents must have the agreement witnessed by their respective SAC or DAD; retired special agents must have the agreement notarized. By signing the agreement, the individual will affirm his or her understanding of the following information:

(a) The criteria for receiving the two-card retired credential.

(b) That the two-card retired credentials do not grant any authority to act on the behalf of NCIS or to exercise any law enforcement authority.

(c) In order for the two-card retired credential to be valid, the individual shall not carry a firearm while under the influence of alcohol or any other intoxicating or hallucinatory drug or substance.

(6) Code 11A will maintain a database identifying the retired special agents who have been issued the two-card retired credentials and the dates of their issuance.

e. Standard retired credential. Special agents who do not meet the qualifications for the two-card retired credentials, or those who do not request the two-card retired credentials, may be

issued a single-card, standard retired credential. The standard retired credential consists of one card that identifies the agency, agency seal, name of bearer, and bearer title. The NCIS seal (in gold and blue) is located on the blue-textured card's right edge. The words "United States of America" are located above the words "Naval Criminal Investigative Service" at the top of the card. The bearer's name is inserted between the lines "This is to certify that" and "is a Retired Special Agent". The bearer's photograph is placed on the card's left edge with "Office of the Director NCIS by order of: The Secretary of the Navy" below the photograph. A completed card will be authenticated and laminated prior to issue.

30-17.2. Retired Badge. A gold colored full-size replica NCIS badge, inscribed on its face with the words "Special Agent" and "Retired" may be purchased. The word "Retired" shall be clearly legible upon examination by an ordinary person and shall be at least the same font type and size as the words "Special Agent". The "Retired" badge does not authorize the exercise of police powers, nor does it grant the recipient any law enforcement authority or privilege, and should not be referred to or displayed as a genuine police badge (18 U.S.C. 716). Government funds may not be used for purchase of a retired badge.

30-17.3. Loss of Retired Credentials. The loss of retired credentials will be handled in the following manner:

a. Loss of Standard retired credentials. In the event that the standard one-card retired credential is lost or stolen, the retired special agent may obtain a replacement by reporting the loss to the DAD Code 11A. Code 11A will then replace the retired credential.

b. Loss of two-card retired credentials. In the event that two-card retired credentials are lost or stolen, the retired special agent shall immediately report the loss to his or her local police department and request that they affect an NCIC entry. Subsequently, the retired special agent shall notify and provide a copy of the police report to the DAD Code 11A. If the two-card retired credentials are not recovered within 15 days, the retired special agent may request new two-card retired credentials. The DAD for Code11A, after a thorough review of the circumstances of the loss, shall determine if the issuance of a new two-card retired credential is justified. If the new two-card retired credentials are issued, they will bear a number different from that of the lost credentials. If the lost credentials are recovered later, they must be forwarded to Code 11A for disposition.

30-18. PROTECTIVE SERVICE PINS

Protective Service Pins (PSPs) are a means of identification issued to authorized personnel for the purpose of providing a unique visual recognition symbol between individuals assigned to a Protective Service Operation/Detail. At no other time is the display of the PSPs authorized. Special agents and other authorized NCIS employees are assigned a set of four serialized pins. Accountability for the PSPs is the responsibility of the person to whom they are issued and due care should be taken in storing them when not in use. The PSPs are controlled items. The same care and custodial responsibility inherent with the NCIS credential and badge are required for the PSPs. Loss of a pin must be immediately reported to the employee's field office or NCISHQ department via the supervisor and to Code 00I. The remaining pins will be returned to Code 11A

via registered mail. The DAD, Code 11A, will provide a replacement PSP set at the recommendation of the SAC or NCISHQ department DAD. The respective field office will return the PSPs to Code 11A, via registered mail, upon retirement or termination of the NCIS employee. Appropriate COMPASS entries will be made by Code 11A.

NCIS - 1 CHAPTER 31
TITLE: Occupational Safety and Health (OSH)
POC: CODE 11B
DATE: NOV 07

31.1 GENERAL
31.2 POLICY
31.3 ENTERPRISE SAFETY APPLICATIONS MANAGEMENT SYSTEM (ESAMS) TRAINING

REFERENCES:
a. OSHA ACT OF 1970
b. DOD INSTRUCTION 6055.1
c. OPNAVINST 5100.23G

31-.1. GENERAL

31-1.1. Purpose.

Establish policies and procedures to administer and facilitate the NCIS OSH program. The policies expressed in this chapter are based on the Occupational Safety and Health Administration (OSHA), Department of Defense (DOD) and Department of the Navy regulations (DON), which are published in references (a) through (c).

31-1.2. Applicability.

This chapter is applicable to all personnel assigned to the NCIS according to specific job duties and work environment. This chapter does not apply to NCIS contractor personnel; all contractor personnel must adhere to polices and procedures contained in their contract.

31-1.3. Responsibility for Compliance.

All NCIS employees are responsible for compliance with this chapter and other regulations regarding the OSH program. Code 11B Deputy Assistant Director for Acquisition and Logistics, NCIS Code 11B exercises agency oversight of the NCIS OSH program.

31-2. POLICY

The safety and health of our employees is one of the highest priorities of the DON and the NCIS. The effectiveness of the OSH program depends on the support and communication of management, supervisors and employees. Everyone must be capable of recognizing hazards in the workplace and each must understand their roles and responsibilities. Supervisors will make the safety and health of all employees an integral part of his/her regular management functions. Every employee will adhere to established

DoD, DON and NCIS OSH policies, procedures and training requirements. Participation by all employees is essential to ensure the effectiveness of the safety program. Employees must report all injuries and unsafe/unhealthy working conditions to their supervisor. Corrective measures will be taken and there will be no organizational retribution or retaliation against employees that report safety and health concerns. Safety is everyone's responsibility and all employees will be held accountable for participating in this program. NCIS has established a Safety Council comprised of representatives from each Field Office to assist in the implementation of the OSH program. The Safety Council will meet on an annual basis.

31-3. ENTERPRISE SAFETY APPLICATIONS MANAGEMENT SYSTEM (ESAMS) TRAINING

31-3.1 Overview.

Safety is one of the top 5 issues delineated by the Secretary of the Navy (SECNAV) for the DON. Safety awareness and mishap reduction are priorities within the safety program. Reference (c) requires all DON personnel complete safety awareness training by using the ESAMS program. The ESAMS safety awareness training program is compliant with current OSHA and Navy Occupational Safety and Health (NAVOSH) standards and training requirements. NCIS will conduct all safety awareness training through ESAMS.

This training provides essential and invaluable information required for all supervisors and employees. Training modules will explain in detail the requirements, responsibilities and procedures for all safety related programs and reports for NCIS employees.

31-3.2 Alternate Training.

If electronic access to ESAMS is not available, supervisors or safety representatives will provide required safety training material(s) in hard copy form to employees. Completed hard copy training material(s) must be returned to the supervisor or safety representative and the supervisor or safety representative is responsible for entering employee completed training information into the ESAMS program.

31.3.3. Training Modules

OSH training is specific to each individual's duties and work environment. The training listed below is not all inclusive within the ESAMS program. There are 36 web-based training modules concerning safety and security available on-line via ESAMS i.e. Bloodborne Pathogen, Back Injury, Fire Prevention, etc. that may be accessed and utilized if desired by all NCIS personnel. The following training is required as indicated:

TITLE	WHO	FREQUENCY	ESTIMATED COMPLETION TIME
Safety Orientation ***(NOTE 1)***	Supervisors / All Employees	One Time	2 Hr
Ergonomics	All Employees	One Time	1 Hr
Personal Protective Equipment (PPE)	1810/1811, Armory personnel, Tech Scvs & Code 11A	One Time	1 Hr
Asbestos Awareness	All personnel in a confirmed asbestos containing Bldg & Code 11A	Annually	1 Hr
Lead Awareness	All personnel in a confirmed lead containing Bldg, armory personnel & Code 11A	Annually	1 Hr
Hearing Conservation ***(NOTE 2)***	Applicable Personnel	Every 5 years	1 Hr
Respiratory Protection	MCRT Personnel, 1811/1810 Afloat & Code 11A	Annually	2 Hr
Hazardous Communication Standard (HCS) ***(NOTE 3)***	GS-15 and Above Tech Scvs, MCRT Personnel, Code 11A	One Time Annually	1 Hr 1 Hr

NOTE 1: Safety Orientation must be completed in FY08; supervisors must complete class #33, non-supervisor must complete class #32. All classes listed above are located in the web training portion of the ESAMS program. All other classes listed, are scheduled for completion in FY09 and thereafter as depicted in the frequency section above.

NOTE 2: Per ref (a), applicable personnel are those that are exposed to noise levels above 84db. Examples: anyone who fires a weapon operates power tools, etc., in the performance of their duties. Personnel exposed to noise levels of 84db to 140 db are

required to wear a minimum of one level of hearing protection. Anyone exposed to noise levels above 140db are required to wear two levels of hearing protection. **All NCIS personnel will wear 2 levels of hearing protection while firing weapons (regardless of range location).**

NOTE 3: The HCS is based on the concept that employees have both a need and a right to know the dangers, properties and protective measures related to any hazardous materials in their workplace. HCS training provides employees with knowledge to better implement and manage communication of hazards in the workplace.

31-3.4. ESAMS LOGIN INSTRUCTIONS.

Use the following steps to complete ESAMS enrollment:

(Active military personnel assigned to NCIS must call the ESAMS help desk and provide information requested by ESAMS personnel before attempting access.)

a. Access the NCIS INFOWEB / http. //infoweb.ncis.navy.mil/
b. Click on Training
c. Click on On-Line Training Courses
d. Click on Enterprise Safety Applications Management System
e. ESAMS Login page will open to "Welcome to ESAMS"

(1) In the User Name field, enter your Last Name and the last (5) digits of your Social Security number (SSN) without spaces.
Example: last name 12345

(2) The initial password will be the last 5 digits of your SSN.
Example: 12345.

(3) Click on Login.

f. If all required information is entered correctly a new page will open requesting users to change their password. Password must have a minimum of eight letters and one number. Users will be asked to select a security question and then to input your email address. Go to top of page and click "save changes". The NCIS Enterprise Safety Application Management System screen will appear. The login process is complete.

g. Once the login process is completed the NCIS ESAMS main page is open. Select "Web Training" to learn more about the ESAMS functions. Scroll Down the list of classes and click on class #11, ESAMS training for Supervisors (Web or Classroom) then click on basic systems. Guidance within System Basics will help you learn to navigate through ESAMS and complete your required training.

31-3.5. ESAMS Helpdesk.

If ESAMS entry is denied, call the ESAMS help desk at (865) 693-0048. Help desk hours are Monday through Friday from 0700 to 2000 EST, and Saturday between 0930 and 1500 EST. Users should inform the help desk that they are assigned to NCIS, are attempting to Login for the first time, and require assistance.

31-3.6. NCIS Occupational Safety and Health Web page.

An electronic link to the NCIS Occupational Safety and Health web page can be found on the Acquisition and Logistics web page via the NCIS Intranet Web Site. The Occupational Safety and Health web page has current information on safety trends and mishaps as well as links for safety and compensation-related forms and instructions for employees.

NCIS-1 CHAPTER 32
TITLE: VEHICLE MANAGEMENT PROGRAM
POC: CODE 11B
DATE: DEC 07

REFERENCES:
(a) 31 U.S.C. Sections 1344 and 1349
(b) DoD 4500.36-R
(c) DoD Instruction 6055.4
(d) SECNAV M-5210.1
(e) OPNAVINST 5100.12G
(f) OPNAVINST 5102.1D
(g) OPNAVINST 6100.2
(h) MANAGEMENT OF CIVIL ENGINEERING SUPPORT EQUIPMENT (NAVFAC P-300)
(i) NCIS VOYAGER FLEET CARD INTERNAL OPERATING PROCEDURES

APPENDICES:
(1) VEHICLE AND EQUIPMENT OPERATIONAL RECORD (ADMINISTRATIVE AND TACTICAL MOTOR VEHICLES), NAVMC 10627
(2) MOTOR VEHICLE ACCIDENT REPORT, SF 91
(3) STATEMENT OF WITNESS, SF 94
(4) ACCIDENT IDENTIFICATION CARD , DD Form 518
(5) NCIS VEHICLE MAINTENANCE REPORT

(6) VEHICLE INSPECTION CHECKLIST
(7) EMERGENCY VEHICLE INSPECTION CHECKLIST
(8) NCIS VEHICLE HISTORY RECORD
(9) NCIS VEHICLE RECORD FOLDER
(10) DRIVER ASSIGNMENT RECORD

32-1. GENERAL

32-1.1. Purpose. Establish procedures to administer, operate, and maintain NCIS owned or leased vehicles. The policies expressed in this chapter are based on applicable Public Law and DOD and DON regulations, which are published in references (a) through (i).

32-1.2. Applicability. NCIS-1, Chapter 32 is applicable to all NCIS employees including civilian and military personnel. Contractor personnel are not allowed to drive NCIS vehicles, unless specifically authorized by contract and regulation. Vehicles rented under Temporary Additional Duty (TAD) or Temporary Duty Travel (TDY) orders are regulated by the Joint Travel Regulations.

32-1.3. Responsibility For Compliance. All government vehicle operators are responsible for ensuring compliance with this chapter and other regulations regarding safe and prudent use of government vehicles. Deputy Assistant Director for Acquisition and Logistics, NCIS Code 11B exercises agency oversight of the NCIS vehicle management program.

32-2. POLICY

Use of Navy owned or controlled vehicles, including those leased using DoD or DON funds or provided by other government agencies or commercial sources, is restricted to actual performance of official duties. The performance of official duties is not construed to include transportation over all or any part of the routes between domiciles and places of employment unless home-to-work transportation has been authorized.

32-3. ILLEGAL USE PENALTY

Minimum penalties for willfully using, or authorizing the use of a Government owned or leased motor vehicle, for other than official purposes, are stipulated in reference (a). Title 31, Section 1349(b), states: “An officer or employee who willfully uses or authorizes the use of a passenger motor vehicle or aircraft owned or leased by the United States Government (except for an official purpose authorized by Section 1344 of this title) or otherwise violates Section 1344 shall be suspended without pay by the head of the agency. The officer or employee shall be suspended for at least one month and when circumstances warrant, for a longer period or summarily removed from office.” (“Passenger motor vehicle,” relative to illegal use, has been interpreted to mean all types of automotive vehicles). Depending on the facts and circumstances, the criminal sanctions of Title 18, Section 641 might apply to the misuse of a Government motor vehicle. That statute provides for a fine of up to $10,000 and imprisonment for up to 10 years.

32-4. PERMISSIBLE OPERATING DISTANCE

It is usually more economical to use the services of commercial carriers for the transportation of personnel and cargo to destinations outside the immediate area of an activity. Although a one-way distance of 100 miles has been selected as a guide to base permissible operating distances for motor vehicles, such a limited distance is impractical to sustain the dynamic NCIS mission in its expansive areas of responsibility. Under the guidance and control of the Special Agent in Charge (SAC)/Deputy Assistant Director (DAD), NCIS vehicles may operate for any length of time and distance consistent with the mission of NCIS, with due regards for safety and economy.

32-5. HOME-TO-WORK (H-T-W) TRANSPORTATION

a. Public law and DoD/DON policy (references (a), (b) and (i)) permit the use of government-owned vehicles for H-T-W transportation in limited cases and prescribe specific documentation requirements and management controls.

b. H-T-W transportation may be authorized when it is considered essential for the safe and efficient performance of intelligence, counterintelligence, protective services or criminal law enforcement duties (references (a), (b) and (i) apply). The purpose of the trip must be related to the performance of official duties or in connection with activities conducted under official authorization.

c. H-T-W transportation for NCIS must be approved annually by the Secretary of the Navy subject to NCIS' annual internal review to ensure compliance with references (a) and (b). See paragraph 32-5.1 for more information regarding annual reviews. The Director, NCIS delegated authority for each H-T-W approval to the Deputy Directors, Field Executive Assistant Director (EADs), SACs and DADs may further delegate authority for H-T-W approval to SSAs for short time requirements not to exceed 30 days.

d. Examples of duties performed by NCIS personnel which may require use of a government vehicle H-T-W include, but are not limited to, the following:

(1) Duty Agents. Special agents, supervisors and other personnel while assigned as the duty agent or office duty responder. Supervisors shall not be routinely authorize H-T-W transportation unless formally designated as a duty supervisor with orders to respond to duty calls.

(2) Major Crimes Response Teams (MCRT). MCRT personnel while designated as the on-duty section. Members of the MCRT, who are not designated as the on-duty section, shall not automatically receive H-T-W transportation authorization.

(3) Proactive Special Operations Team Members or individuals engaged in similar type of operational activities. Operational activity is anticipated or the member is in a duty status as a duty responder.

(4) Joint terrorism and other task forces while in a duty status only.

(5) NCIS personnel engaged in other operational activity for "official purposes." The term "official purpose" means that a person must perform travel in their official capacity.

32-5.1 Annual Review of H-T-W Authorizations. Reference (b) requires that NCIS will conduct internal reviews of H-T-W authorizations and requires that NCIS maintain a central record system of positions or persons for whom H-T-W vehicles are authorized. The Director must approve this list annually. To accomplish this annually, each SAC will submit through their EAD a list of those positions requiring H-T-W vehicles (per the guidance in the previous paragraph). This report will be forwarded by the EAD to NCIS Code 11B who will prepare a brief for the Director. The following information should be included in the SAC's submission: (1) driver's assignment or position, and (2) reason H-T-W required. Additionally, the Inspector General, NCIS Code 00I will ensure, during periodic field office inspections that field activities are in compliance with guidelines prescribed above.

32-5.2. H-T-W Logs

a. References (a), (b), (i) and (j) require accounting of H-T-W transportation authorizations. Letters authorizing blanket approval for H-T-W transportation are not permitted. Each approving authority shall maintain an electronic log of H-T-W transportation authorizations, for a minimum of three years to establish that all H-T-W transportation was used for official purposes. The electronic log, which only requires entries upon initial assignment of the H-T-W vehicle, and upon termination of the assignment, will include the information required by reference (b) and (h).

(1) Employee Name and Position Title

(2) Passenger carrier identification. (USN number – 7 digits no dash)

(3) Date (MM/DD/YY)/Time (0000-2359) vehicle was taken

(4) Date (MM/DD/YY)/Time (0000-2359) vehicle was returned

(5) Location (city and state) of home where vehicle was taken

(6) Brief circumstances requiring H-T-W transportation

(7) Name of the authorizing official (Last name, First name, Title).

b. An electronic log template has been prepared by NCIS Code 11B2 for use by field offices and codes that normally grant H-T-W transportation. The H-T-W log template can be found on the Acquisition and Logistics web site http://inforweb.ncis.navy.mil/agency/deptwebsites/acqlog/al-index.html.

c. H-T-W logs will be maintained for three years and shall be an inspection item.

32.-5.3 Incidental Use. Under the authority reference (b), incidental use of a home-to-work vehicle may be made during the home-to-duty or duty-to-home trip so long as it does not constitute a substantial increase in the distance of a direct home-to-duty or duty-to-home trip and involves only a brief stop for such routine things as cleaning, prescriptions, grocery items, and the like, that are a common part of any home-to-duty or duty-to-home trip. No passenger pick-up is permitted. The deviation:

a. Must not adversely affect official duties.

b. Must be of reasonable duration and frequency.

c. Must occur only during the employee's personal time.

d. Must not reflect adversely on DoD.

e. Must not create any significant additional cost to DoD.

32-6. PARKING OR GARAGING OF MOTOR VEHICLES

Operational requirements and the safety and security of the motor vehicle are the primary consideration when parking the government vehicle. The parking facilities of other DoD installations or federal, state or local government property shall be used to the fullest extent feasible. Where other federal, state or local facilities are not available, commercial parking facilities may be used. This section does not apply to H-T-W vehicles, although safety and security should always be a consideration.

32-7. ACCIDENT REPORTING AND TRAFFIC SAFETY

32-7.1. DoD policy, as set forth in DoD Instruction 6055.4 (Department of Defense Traffic Safety Program), requires each DoD component to establish and maintain comprehensive traffic safety programs. DoD Instruction 6055.7 (Accident Investigation, Reporting, and Record Keeping) requires investigation of each accident involving a DoD motor vehicle.

a. The Navy Traffic Safety Program, promulgated by reference (f) requires all accidents/mishaps involving Navy vehicles/automotive equipment to be reported in accordance with OPNAVINST 5102.1D.

b. All NCIS motor vehicles shall contain, at a minimum, two copies of the Motor Vehicle Accident Report, SF 91; Statement of Witness, SF 94; and an Accident Identification Card, DD Form 518 and a Federal Employee's Notice of Traumatic Injury and Claim for Continuation of Pay/Compensation, Form CA-1. To properly prepare DD Form 518 the motor vehicle operator will need to contact the local Naval Legal Services Office (NLSO) to obtain the correct address in order to complete the space titled "Any correspondence regarding accident should be addressed to:" Fill in the address of NCISHQ in the space titled: "Organization". NCISHQ address is: 716 Sicard Street SE, Suite 2000, Washington, DC 20388-5380.

32-7.2. Accident/Mishap Reporting. Accidents involving a Navy-owned, leased or rental motor vehicle must be reported via the NCIS Safety Program Environmental Safety Applications Management System (ESAMS) under the Injury, Illness Report Tracking System (IIRTS). It should be noted that IIRTS can only be accessed by supervisors and NCIS safety representatives. Supervisors must be notified of an accident/mishap within 90 minutes from the time the accident/mishap occurred. In addition a GENADMIN must be submitted to the chain of command with copy to NCIS Code 11B2 within three work days. The motor vehicle operator must complete SF 91(Rev. 2-93) (NSN 7540-00-634-4041) Report of Motor Vehicle Accident, for all accidents and when applicable SF 94 (Rev 2-83) (NSN 7540-00-634-4045), Statement of Witness within 30 calendar days of the GENADMIN submission date. The original SF 91 shall be retained by the cognizant office and copies forwarded through the chain of command with a copy to NCIS Code 11B2. Forward any supporting documentation, i.e., Photographs, Official Repair Estimates, Final Repair Receipt(s), Official Law Enforcement Reports, etc. to NCIS Code 11B2.

a. Accident GENADMIN. The GENAdmin must contain, at a minimum, the following information as applicable:

(1) Date of Accident

(2) Time of Accident

(3) Location of Accident

(4) Motor Vehicle Driver complete name (first, middle initial and last name)

(5) Passenger(s) name(s)

(6) The vehicle Make, Model, Year, VIN, and USN number

(7) Identify whether the accident occurred in the Line of Duty? Yes/No.

(8) Did this accident happen during the transit from H-T-W? Yes/No? If the answer is yes, describe the reason for the H-T-W authorization

(9) Injuries? Yes/No? If the answer is yes, provide brief description

(10) Provide a brief description of the accident

(11) Provide a brief description of the damage to the government motor vehicle

(12) Identify the estimated damage amount

(13) Identify whether local law enforcement support was requested and describe the result(s)

(14) Identify whether a citation was issued – Yes/No. If the answer is yes; identify whom and the nature of the citation

(15) Fault / No Fault Determination by SAC/DAD. – Fault or No Fault

b. The motor vehicle driver involved in a government motor vehicle accident will stop immediately; determine whether there are any personal injuries; if necessary, render first aid; notify EMS support and local police. Do not move injured people unless absolutely essential for their protection.

c. Render the accident scene safe; warn other motorists of any existing highway hazard. During hours of darkness or poor visibility, use three reflective warning triangles and/or non-flame producing warning devices to warn other motorists. NCIS personnel are not authorized to purchase, use or store flame-producing flares in government motor vehicles or in parking facilities.

d. Do not express oral or written opinions to accident claimants or their agents concerning the liability, investigation findings, or possibility of claim approval. Complete a DD Form 518 at the scene of the accident, or as promptly as possible thereafter, and provide copies to all persons directly concerned. DD Form 518 provides people involved in an accident with the identity of the government entity authorized to act upon the matter.

e. Complete a SF 91 and SF 94 (when applicable). If a SF 91 cannot be prepared because of injury or death, the next senior person directly responsible for the motor vehicle operations will complete these forms.

f. Comply with state and local laws governing the reporting of motor vehicle accidents. Official reports will be submitted through channels to the appropriate claims officer for review to ensure that the rights of the U. S. Government are not prejudiced by an admission of liability that may obligate the government.

g. Do not leave the scene of the accident except as authorized by a state law enforcement officer or other proper authority.

h. Do not make official accident investigation reports available to a claimant, or to any individual or representative of any non-DoD organization. Clearance must be obtained from the cognizant NLSO or NCIS Code 00L before delivery of any accident report to a third party, including state and local officials.

i. Driver improvement courses are required for:

(1) Military and DoD civilian personnel driving a Government vehicle involved in an “at fault” crash whether on or off government property. The NCIS Safety Officer, NCIS Code 11B2 determines whether or not an accident is at fault based on the facts presented by the accident/mishap report. When an accident results in a vehicle repair cost at or below $1000 and the accident occurred in a parking lot and/or garage (i.e. not in traffic) and where there is no

personal injury, the SAC/DAD will determine if the driver should attend AAA Driver Improvement Program (DIP) training. The decision by the SAC/DAD to waive AAA DIP training is a one-time exception. If the driver has more than one accident that is determined to be "at fault" within a three-year period, regardless of vehicle repair cost, then AAA DIP training is mandatory. The SAC/DAD will counsel the individual regarding the incident.

(2) Per OPNAVINST 1500.12G, enclosure (1), 3b (c), individuals described above driving a government or private vehicle who have been convicted of serious moving traffic violations (e.g., reckless driving, driving while impaired, speeding, following too closely, and failure to yield).

(3) Offenders, military or civilian, must successfully complete a driver improvement course or lose installation-driving privileges.

(4) The Safety Officer, NCIS Code 11B2 will notify the individual if they are at fault. SAC's /DAD's will be notified by the DAD of Code 11B. If the individual or SAC/DAD disagrees with the "at fault" finding, they may appeal that finding via e-mail to the DAD, Acquisition and Logistics, NCIS Code 11B. All appeal decisions made by NCIS Code 11B will be final. All appeals will be endorsed by the SAC/DAD. In all cases of an "at fault" finding, except as noted above, the individual will be required to complete AAA DIP training within 90-days of notification from the Safety Officer NCIS Code 11B2. If training cannot be completed within the required time frame notification must be sent to the Safety Officer, NCIS Code 11B2 stating the reason for noncompliance and an estimated time of completion must be given based on the availability of AAA DIP classes in the individual's locality and operational commitments. Not all OCONUS locations will have the AAA DIP training available. In these cases training will be completed as soon as practical when the individual is in a locality that offers the training.

(5) For military personnel, enter the completion of driver improvement training on page 13 of the member's service record. For civilian personnel, enter the completion of driver improvement training in the individuals local training record. It is the individuals responsibility to notify their private automobile insurance company of the completion of training.

(6) Mail a copy of the AAA DIP training completion certificate attention Safety Officer, NCIS Code 11B2 no later than 10 working days after completion.

(7) AAA DIP training enrollment can be accomplished by:

(a) Telephone or e-mail the ESAMS help desk at (865) 693-0048 and ask to be enrolled in an AAA DIP training class within the applicable locality.

(b) E-mail (b)(6) @hgwllc.com, and info copy the Safety Officer, NCIS Code 11B2 and request to be enrolled in an AAA DIP training class within the applicable locality.

If the above methods are unsuccessful please contact the NCIS Safety Officer at (b)(6) and request assistance.

j. An official accident report must be sent to Commander, Naval Safety Center within 30 calendar days of an accident or mishap involving the operation of a DoD or DON motor vehicle when the accident or mishap:

(1) Involves collisions with other motor vehicles

(2) Pedestrians, or bicyclists when struck by a motor vehicle

(3) Other objects

(4) Personal injury or property damage due to cargo shifting in the motor vehicle

(5) Personal injury in moving vehicles or by falling from moving vehicles

(6) Towing or pushing mishaps

(7) Other injury or property damage

k. Official correspondence will originate from NCISHQ when the accident or mishap meets one or more of the following criteria:

(1) All Government Motor Vehicle (GMV) or Government Vehicle Other (GVO) mishaps resulting in $5000 or more government vehicle or government property damage, and/or injury/fatality of DoD personnel; or a mishap caused by a GMV/GVO resulting in $5000 or more total damage including any private vehicle or private property damage, and/or injuries/fatalities to non-DoD personnel.

(2) A fatality or lost time injury that meets the definition in OPNAVINST 5102.1D, Chapter 3, paragraph 301a (2).

(3) A fatality or injury requiring treatment greater than first aid to non-DoD personnel.

32-8. NCIS MOTOR VEHICLE POLICY AND PROCEDURES

a. Government motor vehicles may only be used for “Official Business”.

b. Citations issued by law enforcement agencies as a result of a moving or parking violation(s) is/are the sole responsibility of the driver of the government vehicle that received the citation(s).

c. The Voyager Fleet Card will be used for all purchases of fuel, oil, tire repair, glass repair, emergency service, preventive and corrective maintenance, in the United States, (reference (i)). The single purchase limit for an item or service on Voyager Fleet Card is $2,500. Expenditures that exceed the $2,500 limit must meet the Federal Acquisition Regulations (FAR) competition requirements and must be approved prior to the expenditure by NCIS Code 11B2. The Voyager Fleet card is normally located in the vehicle key case. The motor vehicle operator is responsible

for using and securing Voyager Fleet Card. The Voyager Fleet Card must never be kept in the vehicle. The Voyager Fleet Card User is responsible to ensure that all transactions are for official government use and may be held liable for failure to do so. In accordance with reference (i) card user's must understand the policies and procedures regarding authorized Fleet Card purchases. Card users, when applicable, complete the Vehicle and Equipment Operational Record NAVMC 10627 (appendix 1); provide transaction receipts and documentation to cognizant APC monthly; sign a Statement of Understanding (SOU); and use self-service gasoline pumps.

d. Seat belts will be worn at all times by all operators and passengers.

e. A valid state driver's license is required for all government motor vehicle operators.

f. Smoking is not permitted in any government motor vehicle.

g. Vehicle operators on a DoD installation and operators of government owned vehicles will not use cell phones unless the vehicle is safely parked or unless they are using a hands-free device. The wearing of any other portable headphones, earphones, or other listening devices (except for hands-free cellular phones) while operating a motor vehicle is prohibited. Use of those devices impairs driving and masks or prevents recognition of emergency signals, alarms, announcements, the approach of vehicles, and human speech. The DoD component safety guidance should note the potential for driver distractions. The prohibitions of this section do not apply to the following:

(1) Emergency use of a mobile telephone, including calls to 911, a fire department, a hospital, an ambulance service provider, or the like.

(2) Use of a mobile telephone by law enforcement and emergency personnel or by the operator of an authorized emergency vehicle, acting within the scope of official duties.

32-9. INSTALLATION AND USE OF WARNING LIGHTS AND SIRENS

a. Warning Indicators. Warning or right-of-way indicators are required in certain motor vehicle and equipment operations. The installation of warning lights and sound devices must comply with local, state and country regulations and laws controlling the application of these devices.

b. Responding to Emergency Calls. NCIS vehicles responding to emergency calls will use sirens and emergency warning devices as set forth in pertinent, local regulations, and civil laws of the locality in which the vehicle is operated. To ensure safe operation, regardless of permissible speed limits, motor vehicles will be operated within the limits dictated by road and/or traffic conditions.

c. Only trained NCIS emergency vehicle operators, as specified in reference (h) (NAVFAC P-300, 3.8.6, c (1)), are authorized to engage in high-speed pursuits. An emergency vehicle operator must decide when there is a true emergency in which there is a high probability of death or serious injury to an individual or significant property loss, and action taken by an emergency

vehicle operator may reduce the seriousness of the situation. Emergency vehicle operators will consult applicable federal, state and local laws in the area of responsibility to ensure that they understand permissible laws and regulations.

32-10. ADMINISTRATION OF GOVERNMENT OWNED OR LEASED VEHICLES ASSIGNED TO NCIS

a. General. The Naval Facilities Engineering Command (NAVFAC) is the program manager for Civil Engineering Support Equipment (CESE). NAVFAC P-300, Management of Civil Engineering Support Equipment, provides general and detailed procedure for the administration, operation, and maintenance of transportation equipment. In accordance with NAVFAC P-300, Navy policy and standards for law enforcement/base security vehicles are regulated by CNO (N09N). The execution of NAVFAC policies and procedures is assigned to Transportation Management Centers (TEMCs). CONUS and European activities are under the cognizance of the Atlantic Division TEMC in Norfolk, Virginia. OCONUS Pacific activities are under the cognizance of the Pacific Division TEMC in Pearl Harbor, Hawaii. Overall vehicle management and coordination for NCIS is under the cognizance of NCIS Code 11B.

b. Allowances. Each NCIS field office has an approved vehicle allowance based on the desired capability level to be reached. The capability levels (CL) are: CL1 100-90%, CL2 90%-80%, CL3 80%-71% and CL4 70% and below. Current policy is that all CONUS field offices will be at CL3, and OCONUS CL1. The number of 1811 billets, military special agent billets, and a percentage of designated support billets determine the allowance. The allowance does not guarantee that allowance quantities will be filled.

c. Inventories. Accurate inventories are essential to the effective management of the NCIS transportation fleet. Dispositions and acquisitions must be recorded promptly. The official Navy inventory, Base Support Vehicle Equipment Management Information System (BSVEMIS), is maintained by NCIS Code 11B. No vehicle will be placed into the NCIS fleet without prior approval from NCIS Code 11B.

d. Registration. Vehicles used by NCIS must have a Navy registration number for identification and liability purposes. This number is required for Navy owned, leased, and special purpose vehicles. Short term rentals, less than 60 days; do not require a Navy number. Navy numbers are assigned by NAVFAC and are obtained from the cognizant TEMC via NCIS Code 11B. Navy owned, leased, and special purpose vehicles are assigned a Navy number prior to or just after delivery. Requests for Navy number(s) for leased vehicles must be forwarded to NCIS Code 11B2, identifying the vehicle by Make, Model, Year, VIN, date received and location. Requests can be made via facsimile, memo or e-mail. A NCIS Vehicle Record will be established and maintained for each vehicle in the NCIS fleet.

e. Acquisitions. NAVFAC is the procurement agency for all Navy owned vehicles. Other commands or activities are not authorized to purchase vehicles without written authorization from NAVFAC. NAVFAC has granted NCIS the authority to commercially lease vehicles to meet operational needs using Operation and Maintenance Navy (O&MN) funds. To purchase

vehicles, Other Procurement Navy (OPN BA-5) funds are required. NCIS does not have an OPN BA-5 budget to purchase vehicles.

f. Navy owned vehicles. Vehicles purchased and distributed by the TEMCs will be distributed on a "fair share" basis. The Navy's owned vehicle allowances are reviewed and approved by NAVFAC every two years. Interim allowance adjustments are authorized and approved through NCIS Code 11B and the cognizant TEMC.

g. NAVFAC has authorized NCIS to lease vehicles to satisfy allowance deficiencies. Leases are contracted through NCIS Code 11B. Special purpose motor vehicles, undercover, surveillance, Major Case Response Team (MCRT), etc., can sometimes be obtained through various means such as seizures or from the Defense Reclamation Management System (DRMS). A vehicle that is being considered for use as a special purpose vehicle must be evaluated. The evaluation consists of:

(1) Diagnostic tests conducted by a certified dealership mechanic.

(2) Age of the vehicle.

(3) Safety equipment installed.

(4) Rated miles per gallon of the vehicle.

(5) Expected usage over a 12-month period.

h. NCIS Code 11B2 and the requestor will use the outcomes of the evaluations to make their recommendation. The recommendation will be forwarded to NCIS Code 11B for final disposition. NCIS Code 11B has the sole authority to determine whether a motor vehicle will be added to the NCIS motor vehicle inventory.

i. The leased vehicle replacement process will start approximately eight months prior to the turn-in date. This process will consider, budget, capability level, specifications, location, etc. Every attempt will be made to have a replacement vehicle under contract and delivered 45-days prior to the turn-in date of the vehicle being replaced.

j. Under no circumstances will a leased vehicle be operated past its turn-in date unless notified by NCIS Code 11B that:

(1) The contract has been extended, or

(2) The contract option year has been exercised.

(b)(6)

(b)(6)

32-11. RECORD KEEPING FOR GOVERNMENT OWNED OR LEASED VEHICLES ASSIGNED TO NCIS

a. General. NCIS field offices will maintain a NCIS Vehicle Record for all government owned or leased motor vehicles and assigned Voyager Fleet Cards. Each field office and NCISHQ department with two or more assigned vehicles will designate a primary and alternate APC to maintain the required NCIS Vehicle Record. Single vehicle records for vehicles assigned to departments will be maintained by NCIS Code 11B2B.

b. Vehicle Record Folder. The NCIS Vehicle Record Folder is a six-part folder that will be used to hold all pertinent motor vehicle specific paperwork. This record will be maintained for as long as the motor vehicle is included in the NCIS motor vehicle inventory. When the motor vehicle is permanently removed from the NCIS inventory, the vehicle record will be retained for a period three years from the year of establishment IAW SECNAV M-5210.1, SSIC 11240.1.a.

c. NCIS Vehicle Record Folder. The NCIS Vehicle Record Folder is comprised of six sections as noted in appendix (9).

OUTSIDE FOLDER LABEL INFORMATION EXAMPLE

A. Make	B. Model
C. Year	D. VIN
E. USN Number	F. Leasing Company
G. Leasing Company Number	

d. Electronic Database File. An electronic database file will be maintained for all motor vehicles in the NCIS fleet. The database files, vehicle record and data elements for each field office and applicable department are electronically linked. The APC for each field office and department is responsible for updating and maintaining the information in their respective database file.

e. Annual Vehicle Site Inventory. All vehicles will be annually sight inventoried by the assigned field office, department or code APC, as applicable, and certified in writing by the cognizant AD, DAD, or SAC. Sight inventory consists of visually verifying the vehicle make, model, and identification number (VIN) located on the vehicle and on the registration with the make, model and VIN listed on the master record listing. NCIS Code 11B2 will produce the

master record listing for each field office, department or code and send it to the applicable APC not later than June of each year. The VINs listed on the master record listing are to be used to conduct the visual comparison. Send results of the annual inventory and certification to NCIS Code 11B2 not later than 45 days after receipt of the master list. Code 11B2 will immediately reconcile the results of all inventory reports, noting and correcting administrative discrepancies as necessary. Corrected documents will be sent to the applicable APC depending on the correction and what it affects.

32-12. PREVENTATIVE MAINTENANCE FOR NCIS OWNED OR LEASED GOVERNMENT VEHICLES

a. An important element of motor vehicle transportation maintenance management is the periodic performance of scheduled preventative maintenance (PM) inspections, lubrication services, and adjustments. The purpose of PM is to keep equipment in a safe and reliable condition, with maximum equipment availability and minimum cost of maintenance and capital equipment.

b. Operator PM. The operator or designated APC, on a monthly basis, should inspect equipment so defects or malfunctions can be detected before they result in serious damage, failure, or accident. Defects detected during these inspections or during the operation of the motor vehicle and equipment, shall be noted and reported to the applicable APC. The operator must stop operation immediately when a deficiency develops that renders the motor vehicle and equipment unsafe or cause damage.

32-13. SCHEDULED PREVENTIVE MAINTENANCE

32-13.1. Qualified automotive inspection personnel shall inspect automotive vehicles for safety and reliability as follows:

a. Vehicle Inspection. The APC is responsible for devising a plan to ensure vehicle inspections are conducted. Each motor vehicle shall be inspected monthly, using appendix (6). Each motor vehicle configured as an emergency vehicle will be inspected weekly using appendix (7). The results of these inspections are to be submitted to the applicable APC upon completion. Completed checklists are filed in Section 3 of the NCIS Vehicle Report Folder. Detected deficiencies must be corrected before returning the vehicle to an operational status.

b. Developing Specifications for Scheduled Inspections and Services. Each NCIS activity or component will develop an inspection specification and schedule in accordance with manufacturer's specifications. The inspection, lubrication, and adjustment functions and frequencies shall be determined from those recommended in the manufacturer's maintenance manual provided with the vehicle.

c. Reliability Inspection. In addition to the monthly and weekly-required inspections, motor vehicles will be inspected and serviced in accordance with the manufacturers prescribed services and service intervals, such as miles or time as set forth in the manufacturer's owner’s manual furnished with the vehicle. Corrective adjustments and repair actions taken as a result of

serviceability inspections shall generally be limited to only those items prescribed by the manufacturer and only to the extent necessary to restore the vehicle to a degree of serviceability consistent with achieving the highest degree of cost effectiveness. The cognizant APC shall authorize repairs only after a through diagnosis and detection of malfunction, wear, or deterioration has been determined. Where the manufacturer specifies optional adjustments, such as "engine tune-up," such adjustments shall be made. Adverse local conditions may require more frequent routine maintenance inspections of a preventive nature to reduce road failure service calls. In such cases, the APC shall determine the requirement and notify NCIS Code 11B.

d. Unscheduled Maintenance Service. Unscheduled maintenance service is the correction of deficiencies reported by the vehicle operator(s) that occur between scheduled safety or other inspections and services prescribed recommended by the manufacturer. Unscheduled maintenance services will generally be limited to the correction of only specific deficiency identified by the operator(s) and confirmed by qualified motor vehicle service and inspection personnel. Other unreported deficiencies observed by the qualified motor vehicle and inspection personnel that affect safety, or could cause damage to the motor vehicle and equipment, must be corrected prior to releasing the vehicle for service.

e. Air Conditioner Maintenance Operations. Chlorofluorocarbons (CFCs) have been identified as ozone depleting substances. Motor vehicle air conditioners have been identified as a controllable source of CFC-12 (Freon R-12) atmospheric emissions. Emissions of ozone depleting substances are prohibited by OPNAVINST 5090 series.

f. Maintenance Recording and Reporting. APCs must use the manufacturers' recommended maintenance as a baseline for motor vehicle maintenance. Other maintenance requirements may apply based on vehicle type and usage which is determined by NCIS Code 11B2.

g. NCIS vehicles that are equipped with equipment such as Networkfleet or similar service will have mileage, preventive maintenance, recall notification, Mpg/Kpg recorded and reported to the applicable APCs via a web-based interface. APCs will ensure when maintenance actions, preventive and/or corrective, are reported to them via Network Fleet or similar service, that the appropriate action is completed within 5 working days of the initial report. A copy of the maintenance alert and a receipt for the preventive and/or corrective maintenance action or other documentation, which shows resolution of the alert, will be kept in Section 4 of the vehicle folder. The number of hours a vehicle is unavailable for use, vehicle downtime, is an important measurement for fleet maintenance. Vehicle downtime is defined as when a vehicle is unavailable for use due to preventive and/or corrective maintenance action(s). Vehicle downtime will be recorded for each vehicle to the nearest hour and reported on the monthly maintenance report. APCs will submit a monthly report, appendix (5), for all vehicles. The monthly vehicle report will be submitted to NCIS Code 11B2 not later than five working days after the last day of the previous month.

32-14. USE OF PRIVATELY OWNED VEHICLES (POV)

32-14.1. The use of POV in the performance of official duties is strongly discouraged. However, POV may be authorized and directed for use in the performance of official duties only

when government owned leased and/or rented vehicles are not available and/or directed for the convenience of the government. An employee who is involved in an automobile accident/incident while using a POV for official duties is provided protection from personal liability under Title 28 U.S. Code sec 2679. The recovery of damages for the employee's damaged POV is identified in JAGINST 5890.1 as up to $2,000 in reimbursement. Reimbursement is contingent upon the following:

a. Travel did not include commuting to or from the permanent place of duty.

b. Loss did not arise from mechanical or structural defect of the vehicle.

c. Travel is not considered to be for the convenience of the government unless it was pursuant to written orders authorizing use for which the claimant is entitled to reimbursement. Travel off an installation without written orders may only be deemed to be for the convenience of the government if the claimant was expressly directed by his superior to use POV to accomplish the mission. The issuance of written orders after the fact raises the presumption that travel was not for the convenience of the government.

d. The claimant must be free from negligence in order to be paid for a collision loss.

e. Travel by the claimant to other buildings on an installation is not considered to be under orders for the convenience of the government.

32-15. COMMERCIALLY LEASED VEHICLES

32-15.1. All CONUS and most OCONUS NCIS field offices have commercially leased vehicles or sub-leased vehicles from NAVFAC as part of their overall allowance. These vehicles have fixed monthly rental costs. To achieve cost effective operations, vehicles must incur a sustained usage.

a. Commercially Leased Vehicle Receipt. A receipt document must be obtained from the contractor's representative when the vehicle is taken into possession by NCIS. The receipt document may take many different forms depending on what the individual contractor uses. The date on the receipt document determines when the billing for that vehicle starts. If a receipt document is not available, immediately notify NCIS Code 11B2 and they will arrange to have a receipt document in place so that the pick-up can take place. Motor vehicles will not be taken into NCIS possession without a receipt document. A copy of the receipt document must be forwarded to NCIS Code 11B within 24 hours of receipt of the motor vehicle. NCIS leased motor vehicles must undergo an inspection prior to pickup from a contractor's representative. Any damage or inoperative features to the leased motor vehicle must be noted and relayed to NCIS Code 11B2 within 24 hours. The original NCIS Leased Vehicle Receipt/Inspection Report is kept in Section 2 of the NCIS Vehicle Record Folder. NCIS Code 11B2 will issue and forward a certificate of origin, USN Number and Voyager Fleet Card to the APC when the motor vehicle receipt document is received.

b. The field office or department APC is responsible for the registration of assigned motor

vehicles. NCIS Code 11B2 will register all vehicles assigned to NCISHQ departments which do not have an assigned APC. NCISHQ departments having an assigned APC are responsible for registering assigned motor vehicles. NCIS Code 11B2 will assist the NCISHQ APC, as necessary, to complete the registration process. If a vehicle is transferred to a field office or to a NCISHQ department from another NCIS field office, the receiving field office or NCISHQ department APC is responsible for ensuring that the motor vehicle registration shows the correct location of the vehicle. The NCIS Vehicle Record Folder, Section 2 will be annotated and the NCIS Vehicle Record Folder will be sent to the gaining APC along with the transferring motor vehicle.

32-16. KEY SETS

32-16.1. The primary key set will be issued to the driver of the assigned motor vehicle at the time of the assignment. The NCIS Vehicle Record Folder, Section 1, Vehicle History and Driver Assignment will be annotated with the date, and recipient of the key set. The driver will print and sign his/her name in the designated space.

a. The primary key set will remain under the control of the APC when for "pool motor vehicles" or, motor vehicles without an assigned driver. The primary key set will be kept in a secure container at all times when not in use. The Primary Key set for "pool vehicles" will be inventoried semi-annually and recorded in the, NCIS Vehicle Record Folder, Section 2, Notes. The inventory must identify the date of the inventory and name of the APC who conducted the inventory.

b. Spare key sets will be kept in a secure container apart from the NCIS Vehicle Record Folder and Primary Key Set. Spare key sets will be kept in a separate key case marked with the following information:

(1) Make

(2) Model

(3) Year

(4) VIN

(5) USN #

c. Spare key sets are used for emergency purposes only.

d. Spare key sets will be inventoried semi-annually and annotated in the NCIS Vehicle Record Folder, Section 2, Notes. The inventory must identify the date of the inventory and name of the APC who conducted the inventory.

e. When a spare key set is issued, the NCIS Vehicle Record Folder, Section 2, Notes will be annotated with the date, name of the APC, recipient and the reason for issue. The recipient will

print and sign his/her name at the end of the Notes entry in the NCIS Vehicle Record Folder.

f. The spare key set will be returned to the APC within 96 hours or receipt of a new primary key set which ever occurs first. The NCIS Vehicle Record Folder, Section 2, will be annotated with the date the key set was returned, name of the APC who received the key set.

g. If the vehicle is transferred to another field office or department both key sets will be sent with the vehicle. The receiving field office or department will inventory the key sets upon receipt and annotate the NCIS Vehicle Record Folder, Section 2, Notes.

h. When the vehicle is returned to the leasing company both key sets will be returned with the vehicle. NCIS Vehicle Record Folder, Section 2, Notes, will be annotated.

32-17. COMMERCIALLY LEASED VEHICLE RETURN

32-17.1. The length of the contract and the date that the vehicle was actually received minus one day determines the date that a vehicle is scheduled for turn in. The following procedures must be followed to successfully complete a motor vehicle return:

a. Notification will be given by the acquisition officer to the leasing company of intent to return the vehicle. Normally this occurs 45 days or sooner prior to the end of the contract.

b. NCIS Code 11B2 will notify the cognizant APC of the intended turn-in of the affected vehicle. This will occur not less than 60 days from the turn-in date.

c. Scheduling of the turn-in inspection will be accomplished not later than 30 days prior to the actual turn-in date. NCIS Code 11B2 will send a vehicle listing to the leasing company with the following information via e-mail:

(1) Make

(2) Model

(3) VIN

(4) Color

(5) Mileage

(6) USN Number

(7) Leasing Company Control Number

(8) APC/POC & Telephone #

(9) Exact address of vehicle location

(10) Contract Number.

d. The inspection date is automatically set at 15 working days prior to the turn-in date. If that date falls on a weekend or holiday the date will be the working day prior to the weekend or holiday.

e. Voyager Fleet Cards will be automatically be cancelled on the turn-in date by NCIS Code 11B2.

f. The leasing company will contact the APC/POC to schedule the actual inspection. If the leasing company does not schedule an inspection, within 5 working days after the initial Email from NCIS Code 11B2; a second request to schedule a turn-in inspection will be initiated by the APC/POC and sent to the leasing company. NCIS Code 11B2 will be notified of the second request via e-mail. The applicable APC must notify NCIS Code 11B2 via e-mail if the leasing company does not contact them within 48 hours after the second request. NCIS code 11B2 will resolve all turn-in scheduling conflicts. All telephone conversations and correspondence will be recorded in the Vehicle History Record, Section 2, Notes.

g. NCIS leased vehicles must undergo a turn-in inspection prior to release to a contractor's representative. It is imperative that all vehicles slated for turn-in be thoroughly inspected. Vehicles will be “detailed” prior to any turn-in inspection. Every attempt will be made to remove and/or repair small dents and dings, and scratches. All fluids will be checked and topped off, tires checked for wear; if there are bald spots or unusual wear patterns the tires will be replaced. All government property must be removed from the vehicle prior to the inspection date. Turn-in inspection preparations should start not less 60 days prior to the pick-up date.

h. The APC for the field or department will accompany the contractor’s representative during the turn-in inspection, noting any item(s) that are in dispute. The contractor who performs the inspection will provide a copy of the completed inspection to the applicable APC upon completion of the inspection. The NCIS Vehicle Inspection Checklist is to be used to record the results of the NCIS vehicle inspection if the contractor’s representative does not use a hard copy. The contractor’s inspection report, NCIS Vehicle Inspection Report, and photographic evidence will be filed in Vehicle History Documents Section 2, of the Vehicle History Record.

i. Any damage to leased vehicles, which falls within the area of “unusual wear and tear,” which includes oil not having been changed or vehicle fluids not being topped off, worn tires, scratches, dents, etc. will result in charges for both material(s) and labor, needed to affect the repair. If during the inspection, subjective damage is noted, an accurate description(s) of the damage is required. An example would be if there were cracks in the windshield, where the crack is located, what the length of the crack is. Photographs, standard print film or digital image, of the damage would prove helpful should a dispute arise between the leasing company and NCIS. Accurate descriptions and photographic evidence provides NCIS with a basis for rebuttal. Digital images may be transmitted via e-mail followed by a disc copy.

j. Within 24 hours of the completion of the vehicle inspection by a contractor's representative:

(a) The license plates will be removed from the vehicle and returned to the issuing Department of Motor Vehicles by a traceable means.

(b) Vehicle registration cancelled by a traceable means.

(c) Destroy the Voyager Fleet Card.

(d) Send an e-mail with the card number to Code 11B2 stating that the card has been destroyed and the Voyager Fleet Card is to be cancelled.

k. These actions will be recorded in Section 2 of the Vehicle History Record. Upon receipt of the e-mail, Code 11B2 will cancel the listed Voyager Fleet Card and send a copy of the cancellation to the applicable APC for enclosure in Section 2 of the Vehicle History Record.

l. No vehicle will be surrendered to the contractor's representative without obtaining a pick-up receipt. A copy of the signed pick-up receipt will be filed in Section 2 of the Vehicle History Record. Notification of vehicle pick-up will be sent to NCIS Code 11B2 within 24 hours of the actual vehicle pick-up via e-mail and a copy of the actual pick-up receipt will be mailed to NCIS Code 11B2 within 48-hours. NCIS Code 11B2 will remove the vehicle from the BSVEMIS upon receipt of the copy of the turn-in receipt. The turn-in receipt will be annotated with the date that the vehicle was removed from BSVEMIS and the printed name of the person who effected the removal. The turn-in receipt will be filed in the COR contract folder.

32-18. DISPOSITION

Navy Owned motor vehicles determined to be unserviceable are normally turned into DRMS. Motor vehicles considered to be unserviceable will be reported to NCIS Code 11B2 for disposition instructions. The normal life expectancy for a Navy owned motor vehicle is 6 years and/or 72,000 miles. Disposition documents will be filed in the NCIS Vehicle Record Folder Section 2. The entire NCIS Vehicle Record Folder will be sent to NCIS Code 11B2 NLT 72 hours after disposition. NCIS Code 11B2 will remove the vehicle from the BSVEMIS upon receipt of the NCIS Vehicle Record Folder. The NCIS Vehicle Record Folder Section 2 will be annotated with the date that the motor vehicle was removed from BSVEMIS and the printed name of the person who effected the removal.

000752

APPENDIX (5) NCIS VEHICLE MAINTENANCE REPORT

REPORTING FIELD OFFICE:								
TOTAL VEHICLES REPORTED:							**MONTHLY / WEEKLY VEHICLE**	**VEHICLE DOWNTIME**
					PREVENTIVE MAINTENANCE	**CORRECTIVE MAINTENANCE**	**INSPECTION COMPLETED (YES / NO)**	**(FULL HOURS ONLY ROUND UP)**
VEHICLE LOCATION (FO / RA / RU)	**VEHICLE USN NUMBER**	**STARTING MILEAGE**	**ENDING MILEAGE**	**TOTAL MONTHLY MILEAGE**	**COMPLETED (DESCRIBE)**	**COMPLETED (DESCRIBE)**	**A "no" response requires an explanation.**	

000753

APPENDIX (6): VEHICLE INSPECTION CHECKLIST

TO BE COMPLETED NOT LATER THAN THE FIRST FRIDAY OF EACH MONTH AND RETURNED TO YOUR AGENCY PROGRAM COORDINATOR (APC)

USN NUMBER	MAKE	MODEL	LICENSE #	MILEAGE	DRIVER		
1.VEHICLE EXTERIOR		SAT	UNSAT	4. DATED ITEMS:		SAT	UNSAT
A. OVERALL CLEANLINESS / DAMAGE					a. SAFETY INSPECTION		
B. BODY	a. RF DOOR				b. REGISTRATION		
	b. RR DOOR				c. DOD STICKER - (if required)		
	c. LF DOOR				d. LICENSE PLATES		
	d. LR DOOR			5. REQUIRED ITEMS:			
	e. TRUNK / TAILGATE			* Voyager Fleet Card *CANNOT*	a. SF 91- (2 COPIES)		
	f. HOOD			be kept in the vehicle.	b. DD 518- (2 COPIES)		
	g. GRILL				c. VOYAGER CARD * & BROCHURE		
	h. ROOF				d. NCIS PLACARD		
	I. BUMPERS F / R				e. SF 94 - (2 COPIES)		
	j. RUST			6. VEHICLE INTERIOR:			
	k. OTHER						
C. GLASS	a. ALL			A. DASH	a. GAUGES - FUNCTIONAL		
D. MIRRORS	a. ALL – INTERIOR / SIDE				b. DASH & INTERIOR ILLUMINATION		
E. TIRES / RIMS	a. ALL AND SPARE				c. WARNING FLASHERS		
	b. PRESSURE				d. RADIO - FUNCTIONAL		
2. ENGINE CONDITION					e. HORN - FUNCTIONAL		
A. OVERALL CLEANLINESS / DAMAGE				B. HEAT - A/C - FAN	a. OPERATION		
B. FLUIDS	a. OIL				b. DEFROST - FRONT / REAR		
	b. TRANSMISSION			C. LIGHTS	a. LOW BEAM		

000754

	c. WINDSHIELD WASHER				b. HIGH BEAM		
	d. BRAKE				c. TURN SIGNALS		
	e. POWER STEERING				d. HAZARDS		
	f. ENGINE COOLANT				e. BACK-UP LIGHT		
	g. LEAKS				f. PARKING LIGHTS		
C. BELTS	a. ALL				g. BRAKE LIGHTS		
D. BATTERY	a. CABLES				h. INTERIOR LIGHTS		
	b. CONNECTIONS			D. INTERIOR / CLEANLINESS	a. SEATS - FUNCTIONAL		
	c. CHARGE INDICATOR				b. FLOOR / TRUNK		
E. WIPERS	a. FRONT/REAR				c. HEADLINER		
3. SAFETY EQUIPMENT				DESCRIBE ALL DISCREPANCIES: (use back if needed)			
	a. ROADSIDE EQUIPMENT KIT						
	b. FIRE EXTINGUISHER / DATE / FULL						
	c. AIRBAG SYSTEM						
	d. SEAT BELT FUNCTION CHECK (ALL)						
A. BRAKES	a. COLD / HOT CHECK						
	b. PARKING BRAKE						

APPENDIX (7): EMERGENCY VEHICLE INSPECTION CHECKLIST

000756

TO BE COMPLETED WEEKLY NOT LATER THAN 1200 THE FIRST WORKING DAY OF THE WEEK
RETURN SHEET TO YOUR AGENCY PROGRAM COORDINATOR (APC)

USN NUMBER	MAKE	MODEL	LICENSE #	MILEAGE	DRIVER		
1.VEHICLE EXTERIOR		SAT	UNSAT	4. DATED ITEMS:		SAT	UNSAT
A. OVERALL CLEANLINESS / DAMAGE					a. SAFETY INSPECTION		
B. BODY	a. RF DOOR				b. REGISTRATION		
	b. RR DOOR				c. DOD STICKER - (if required)		
	c. LF DOOR				d. LICENSE PLATES		
	d. LR DOOR			5. REQUIRED ITEMS:			
	e. TRUNK / TAILGATE			* Voyager Fleet Card *CANNOT*	a. SF 91- (2 COPIES)		
	f. HOOD			be kept in the vehicle.	b. DD 518- (2 COPIES)		
	g. GRILL				c. VOYAGER CARD * & BROCHURE		
	h. ROOF				d. NCIS PLACARD		
	I. BUMPERS F / R				e. SF 94 - (2 COPIES)		
	j. RUST			6. VEHICLE INTERIOR:			
	k. OTHER						
C. GLASS	a. ALL			A. DASH	a. GAUGES - FUNCTIONAL		
D. MIRRORS	a. ALL - INTERIOR / SIDE				b. DASH & INTERIOR ILLUMINATION		
E. TIRES / RIMS	a. ALL AND SPARE				c. WARNING FLASHERS		
	b. PRESSURE				d. RADIO - FUNCTIONAL		
2. ENGINE CONDITION					e. HORN - FUNCTIONAL		
A. OVERALL CLEANLINESS / DAMAGE				B. HEAT - A/C - FAN	a. OPERATION		
B. FLUIDS	a. OIL				b. DEFROST - FRONT / REAR		
	b. TRANSMISSION			C. LIGHTS	a. LOW BEAM		

	c. WINDSHIELD WASHER				b. HIGH BEAM		
	d. BRAKE				c. TURN SIGNALS		
	e. POWER STEERING				d. HAZARDS		
	f. ENGINE COOLANT				e. BACK-UP LIGHT		
	g. LEAKS				f. PARKING LIGHTS		
C. BELTS	a. ALL				g. BRAKE LIGHTS		
D. BATTERY	a. CABLES				h. INTERIOR LIGHTS		
	b. CONNECTIONS			D. INTERIOR/CLEANLINESS	a. SEATS - FUNCTIONAL		
	c. CHARGE INDICATOR				b. FLOOR / TRUNK		
E. WIPERS	a. FRONT/REAR				c. HEADLINER		
3. SAFETY EQUIPMENT				DESCRIBE ALL DISCREPANCIES: (use back if needed)			
	a. ROADSIDE EQUIPMENT KIT						
	b. FIRE EXTINGUISHER / DATE / FULL						
	c. AIRBAG SYSTEM						
	d. SEAT BELT FUNCTION CHECK (ALL)						
A. BRAKES	a. COLD / HOT CHECK						
	b. PARKING BRAKE						

000757

APPENDIX(8): NCIS VEHICLE HISTORY RECORD

VEHICLE IDENTIFICATION SECTION

Make: _____ Registration Date:
_____

Model: _____ License Plate Number:
_____

Year: _____ State Inspection Date:
_____

VIN: _____ Vehicle Emergency Kit (Yes/No):
_____

Color: _____ Serial Number:
_____

USN Number: _____ Date Inspected:
_____

VEHICLE RECEIPT AND TURN-IN SECTION

Leasing Company Name: Leasing Company Unit ID Number:
_____ _____
Date Vehicle Received:
_____
Address: _____
_____ Date Vehicle Inspected For Turn-In:
_____

Telephone Number: _____ Date Vehicle Turned In:
_____

POC: _____ Date Tags Returned:
_____

VOYAGER CARD DATA SECTION

	CURRENT	PAST
Voyager Card #:	_____	_____
Expiration Date:	_____	_____
Date Received:	_____	_____
Date Replaced:	_____	_____
Card PIN:	_____	Date Voyager Card Cancelled: _____

Card Limit: _____

EMERGENCY VEHICLE DATA

Emergency Equip Installed: _____

Date Installed: _____

Cost of Equipment: _____

Cost of Installation: _____

APPENDIX (9): NCIS VEHICLE RECORD

SECTION 1: VEHICLE HISTORY AND DRIVER ASSIGNMENT

A. NCIS VEHICLE HISTORY RECORD
B. DRIVER ASSIGNMENT HISTORY RECORD (Appendix 10)

SECTION 2: VEHICLE HISTORY DOCUMENTS

A. COPY OF RECEIPT DOCUMENT AND NCIS INSPECTION DOCUMENT.
B. COPY OF CERTIFICATE OF ORIGIN (WHEN APPLICABLE).
C. COPY OF BSVEMIS NAVY MOTOR VEHICLE MASTER RECORD, 4920
D. COPY OF REGISTRATION DOCUMENTS - STATE, LOCAL, DON ETC.
E. COPY OF TURN-IN DOCUMENT AND NCIS INSPECTION DOCUMENT.
F. COPY OF TURN-IN DAMAGE ASSESSMENT DOCUMENT FROM LEASING COMPANY.
G. COPIES OF ALL Emails CONCERNING THE VEHICLE.
H. NOTES PAGE – RECORD OF TELEPHONE CONVERSATIONS CONCERNING THE VEHICLE (WHO, WHAT, WHEN, WHERE, SUBJECT, RESOLUTION, ETC.)

SECTION 3: VEHICLE INSPECTION

A. COMPLETED MONTHLY NON-EMERGENCY VEHICLE CHECKLIST.
B. COMPLETED WEEKLY EMERGENCY VEHICLE CHECKLIST.

SECTION 4: VEHICLE MAINTENANCE

A. COPY OF REQUIRED MAINTENANCE FROM OWNERS MANUAL.
B. COPIES OF ALL MAINTENANCE ACTIONS COMPLETED – PREVENTIVE AND CORRECTIVE.
C. COPY OF NETWORKFLEET/NETWORKCAR ALERTS.

SECTION 5: VOYAGER FLEET CARD

A. COMPLETED NAVMC 10627 FORMS WITH ATTACHED RECEIPTS.
B. MONTHLY EXCEPTION TRANSACTION RECORD.
C. DRIVER STATEMENTS FOR EXCEPTIONS (MISC, FOOD, SUPER, SUPER+, FULL SERVICE AND ODOMETER).

SECTION 6: VEHICLE ACCIDENT HISTORY DOCUMENTS

A. COPY OF ACCIDENT GENADMIN.
B. COPY OF SF 91 and SF 94.
C. COPY OF REPAIR ESTIMATE AND FINAL REPAIR COST.
D. PHOTOGRAPHS OF VEHICLE DAMAGE.

APPENDIX (10): DRIVER ASSIGNMENT HISTORY RECORD

GENERAL RECORD (Type II)
OPNAV FORM 1500-31 (10-60)

0107-LF-701-0000 PERIOD COVERED: FROM TO

TITLE

DRIVER ASSIGNMENT HISTORY RECORD

COLUMN CAPTIONS Make: Model: VIN:	DATE ASSIGNED	DATE RETURNED	EVOC QUALIFIED	VOYAGER CMD USSR					
NAME (LAST/FIRST)	M/D/Y	M/D/Y	Y/N	Y/N					

NCIS-1, CHAPTER 33
RADIO COMMUNICATIONS
EFFECTIVE DATE: FEBRUARY 2015

TABLE OF CONTENTS **PAGE**

REFERENCE

(a) DoD Instruction 5000.64, Accountability and Management of DoD Equipment and Other Accountable Property, May 19, 2011

33-1. Purpose. This chapter establishes policy and procedures governing the use and stewardship of communications equipment by NCIS personnel. Appendix A contains a glossary of common radio communications terms.

33-2. Policy. The provisions in this chapter apply to all NCIS personnel who use or manage NCIS radio communication equipment. For questions about this policy or NCIS's radio communications program, please contact the Office of Technical Services (OTS) at (b)(6) @navy.mil.

a. OTS is responsible for meeting the radio communications needs of NCIS worldwide. Providing radio communications is accomplished by leveraging existing Navy and Marine Corps radio infrastructures, using established law enforcement networks, and by developing dedicated NCIS systems.

b. For most non-expeditionary communications requirements, OTS will coordinate with local Navy/Marine Corps Enterprise Land Mobile Radio (ELMR) communications managers to ensure local offices have the necessary equipment, talk channels, and interoperability with commands. In areas where the ELMR trunking radio network has not been implemented, NCIS radio needs will be met with dedicated NCIS radio systems. In these instances, OTS will provide fixed repeater networks, as required. The OTS also maintains a suite of quick-deploy radio kits that can be used to conduct operations beyond the range of fixed repeater systems.

33-3. Cancellation. NCIS-1, Chapter 33, April 2008.

33-4. Chapter sponsor. Criminal Investigations and Operations, Code 23.

33-5. System descriptions. OTS capabilities change regularly. See OTS' Lighthouse page for the most current information.

(b)(7)(E)

c. Cellular-data based communications. OTS can supply encrypted, smartphone-based communications for groups requiring additional stealth and enhanced operational awareness.

d. Overseas environments. Operating frequencies are coordinated with the host country and are assigned to NCIS by DoD area frequency coordinators. Frequencies and operating procedures will vary greatly from area to area. To obtain the most current operational information for your area of responsibility, coordinate with OTS.

33-6. Equipment

a. Inventory. In compliance with reference (a), OTS maintains an inventory of sensitive equipment. This includes a list of all radio equipment assigned to field components. By January 31 of each year, field offices must send OTS (via (b)(6) @navy.mil) a comprehensive inventory—including make, model, serial number, and location—of all radio assets issued for operational and administrative use. The Radio Inventory Sheet is available on OTS's Lighthouse page. OTS must be notified when radios are permanently transferred from one office to another.

b. Equipment loss. Lost or stolen communications equipment must be reported immediately to supervisors and OTS (via (b)(6) @navy.mil). In some instances, OTS may deactivate the device remotely to maintain operational security. After the email notification, submit a completed form DD 200 (found on Lighthouse) to Code 11B and the NCIS Inspector General.

c. Maintenance and repair. Issues pertaining to the maintenance and repair of NCIS radio communications equipment must be referred to OTS for guidance. Repairs will be made or coordinated by OTS personnel. The issuance of surveillance kits, magnetic mount antennas, and other expendables and accessories must be coordinated with OTS.

d. Requests. Direct requests for additional communications equipment to OTS. If it becomes necessary for NCIS to communicate with an outside agency, generally that agency must provide the equipment. Many state and local public safety organizations have moved radio operations to (b)(7)(E) standard-issue equipment provided to NCIS field units. If long-term interagency communications are required, written permission from the outside agency may be required, based on their policies.

33-7. Radio Communications

a. Radio etiquette. Radio traffic should be conducted in a businesslike manner. Short, declarative statements followed by distinct pauses improve intelligibility and lessen confusion. It may be necessary to use a phonetic alphabet to convey key information. When using a phonetic spelling, choose commonly understood words that emphasize the first letter (e.g., alpha for "a," bravo for "b").

(b)(7)(E)

c. Limitations. It is highly recommended that thorough radio checks be conducted prior to operations. These checks should be conducted where the operation will take place, when possible. Local OTS detachments can assist field offices with planning and testing. VHF and UHF radio waves provide line-of-sight communications that, in principle, travel in straight lines. UHF and VHF radio waves can penetrate solid materials (a building wall, for example), but the signal is degraded. Each additional obstruction will attenuate the signal more until there is no signal remaining. This is generally referred to as a dead spot. Mobile phones and other radios respond best to signals originating from outside a building when the transceivers are near an outside wall or window. As a general rule, a radio signal will not penetrate more than three walls and still be useable. Other areas that will impede radio communications are underground parking structures, dense urban centers, and areas abutting large hills.

d. Portable/handheld operations. Using handheld radios from inside a vehicle greatly attenuates the transmitted signal due to absorption by the metal structure of the vehicle. For optimum operation and to greatly improve the communications range, mount a magnetic antenna outside the vehicle and connect to the handheld's antenna port. When using any transmitter or receiver, the antenna should be as far away from metal objects as possible and should never be operated within a completely enclosed metal structure.

e. Specialized communications. OTS maintains a variety of specialized communications devices that are available for issue to the field. These items are generally provided in support of deployments but are also available for operational scenarios that require extended communications capabilities. Some equipment may interoperate with other law enforcement entities. Access to non-NCIS networks may require permission to operate on these systems prior to use.

APPENDIX A
GLOSSARY OF COMMON TERMS

1. Advanced encryption standard (AES). Specification for standard 256-bit electronic encryption.

2. Antenna. Device to radiate radio frequency (RF) energy into space as well as to collect RF energy from space.

3. Attenuate. To reduce signal strength usually by absorption or reflection.

4. Carrier. The RF energy used to transmit information from one location to another.

5. Channel. A portion of the RF spectrum allocated for particular use (i.e., voice communications).

6. Control head. An under-the-dash mounted unit that contains the controls for a mobile unit. It may also contain a touch tone keypad and with siren controls.

7. Duplex operation. Simultaneous transmitting and receiving on two different frequencies.

8. Encryption. An algorithm used to make voice messages unintelligible to outside parties.

9. Handheld unit. Portable radio.

10. Key loader. A handheld device used to load cipher keys in to encryption-capable radios.

11. Mobile unit. Radio specifically manufactured to be mounted in a vehicle.

12. (b)(7)(E)

13. Portable repeater. A small radio device that extends the talk range of mobiles and portable radio equipment that can be temporarily located overlooking an operation area.

14. Repeater. A radio transceiver that simultaneously transmits what it receives.

15. Simplex operation. Transmitting and receiving on the same frequency (but not simultaneously). Commonly referred to as “talk around.”

16. Trunking. A radio system that consists of a series of repeaters that handles communications in manner that is analogous to a cellular telephone network.

17. Ultra high frequency (UHF). Radio frequencies between (b)(7)(E)

18. Very high frequency (VHF). Radio frequencies between

NCIS-1, CHAPTER 34
FIREARMS, INTERMEDIATE WEAPONS AND USE OF FORCE
EFFECTIVE DATE: FEBRUARY 2014

Table of Contents

References:
(a) SECNAVINST 5500.29c of 27 Aug 2003, Use of Deadly Force and the Carrying of Firearms by Personnel of the Department of the Navy in Conjunction with Law Enforcement, Security Duties and Personal Protection
(b) SECNAVINST 5430.107 of 28 Dec 2005, Mission and Functions of the Naval Criminal Investigation Service
(c) Title 10 U.S.C. § 1585 Carrying of Firearms
(d) DoD Directive 5210.56 of 1 Apr 2011, Carrying of Firearms and the Use of Force by DoD Personnel Engaged in Security, Law and Order, or Counterintelligence Activities
(e) 18 U.S.C. § 922(g)(9) Unlawful Acts
(f) 49 U.S.C § 46505 Carrying a Weapon or Explosives on an Aircraft
(g) 49 U.S.C § 46303 Carrying a Weapon
(h) 49 CFR § 1544 Aircraft Operator Security: Air Carriers and Commercial Operators
(i) NCIS-3, Chapter 41 of Sep 2009, Response Protocol for Major Incidents Involving NCIS Personnel
(j) JAGINST 5800 7F of 26 Jun 2012, Manual of the Judge Advocate General

34-1. Purpose. This chapter establishes policy and procedures regarding lawful use of force, carrying, and using firearms and intermediate weapons. This chapter includes policy regarding firing range procedures, safety practices, and training requirements.

34-2. Policy. The provisions of this chapter apply to Naval Criminal Investigative Service (NCIS) employees authorized to carry firearms and to use intermediate weapons as sworn Federal Government law enforcement officers. This chapter also applies to non-special agent personnel who are engaged in full-time law enforcement, security or

counterintelligence duties and are authorized to carry Government issued firearms. This policy is consistent with the United States Code (USC), Department of Defense (DoD) instructions, Secretary of the Navy (SECNAV) instructions, and Federal rules and regulations governing possession and transportation of firearms, and use of force. When regulatory changes occur, this chapter will be updated.

34-3. Cancellation. The policy documents and other General Administrative documents listed below are cancelled and have been incorporated into this chapter.

a. Gen Admin 11B-0010 of 27 Oct 2008: Transition to the (b)(7)(E)

b. Gen Admin 00I-0008 of 28 Jul 2009: Arming of Reserve Master-At-Arms Personnel.

c. Gen Admin 11C-0020 of 5 Oct 2009: NCIS Policy Document 09-06: Training (TSA – Regulations Regarding Flying Armed by Sworn LEO and Recurring Training).

d. Gen Admin 11C-0022 of 21 Oct 2009: NCIS Policy Document 09-08: Administrative (Personal Weapons Authorized for Official Use).

e. Gen Admin 23A-0007 of 28 Jan 2010: Federal Law Enforcement Officer Flying Armed Procedures.

f. Gen Admin 10B-0053 of 13 May 2010: Training Matters: Updated Guidance for Firearms Qualification Procedures.

g. Gen Admin 10B-0002 of 12 Dec 2012: Non-Special Agent Firearms and Use of Force Training Administrative Requirements.

h. NCIS-1, Chapter 34 of May 2008.

34-4. Chapter Sponsor. NCIS Training Academy, Code 10B.

34-5. Responsibilities

a. All NCIS personnel are accountable for Federal Government issued weapons, ammunition, and credentials; and when issued firearms, or other weapons to demonstrate competency and safety through mandatory training.

b. The special agent in charge (SAC) must ensure their field office is compliant with security, requisitioning, storage, and expenditure reporting of all arms ammunition and explosives (AA&E). SACs must conduct sighting of credentials, firearms, and other intermediate weapons during check-in and check-out events. The NCIS Inspector General (Code 00I) may also sight and inventory firearms, both personal and government-issued, at headquarters directorates and field office components during inspections.

34-6. Authority for NCIS Personnel to Carry Firearms. Consistent with reference (a), special agents are authorized to carry NCIS-approved firearms at all times, while on or off duty, and while on and off installations, aircraft, and ships. Reference (b) requires special agents to carry NCIS approved firearms while on official business, except when in specific "exclusion areas" where special weapons and systems are stored. The commander or commanding officer having responsibility for the "exclusion area" will determine the need for a special agent to carry firearms in these areas.

a. The statutory authority for carrying firearms by special agents is found in reference (c), which states: "Under regulations to be prescribed by the Secretary of Defense, civilian officers and employees of the DoD may carry firearms or other appropriate weapons while assigned investigative duties or such other duties as the Secretary may prescribe."

b. Reference (d) implements those provisions that govern the carrying of firearms and the use of deadly force by DoD military and civilian personnel performing law enforcement and security duties.

c. NCIS policy and regulations refine the authority discussed in reference (a).

d. NCIS is also guided by reference (e), the DoD rules on the implementation of the Lautenberg Amendment to the Gun Control Act of 1968. The Lautenberg Amendment makes it a felony to sell or dispose of firearms or ammunition to an individual who has been convicted of a domestic violence misdemeanor. The Amendment also criminalizes the possession of a firearm or ammunition by such an individual. There are no exceptions for military members or civilian law enforcement personnel. Thus, it is a crime for military members or civilian employees who have been convicted of domestic violence misdemeanors to possess a firearm for any reason. All personnel with these convictions are required to complete DD Form 2760, "Qualification to Possess Firearms or Ammunition."

34-7. Definitions

a. Firearms. Weapon from which a shot is discharged by gunpowder, i.e. handgun, rifle, shotgun, submachine gun, machine gun.

b. Intermediate Weapons. Weapons other than firearms, designed to establish and maintain physical control when use of force is required, but deadly force is not appropriate. Intermediate weapons are not intended to replace firearms since they may not suffice when the use of lethal force is necessary.

c. Use of Force. When the special agent or non-agent has a reasonable belief that the subject of such force poses an imminent danger of death or serious physical injury to the special agent, non-agent, or another person. The standard that will be used to measure the agent or non-agent's actions will be that of "objective reasonableness." The shooter's

use of deadly force will be viewed in light of the facts and circumstances confronting him or her at the time of the incident.

34-8. Issuing Firearms. NCIS will issue firearms to special agents successfully completing the required qualifications course. Firearms may be issued to selected non-special agent personnel meeting the qualifications listed below who comply with reference (a) requirements; and who have received authorization by the Director, NCIS.

a. Reference (d) provides that other accredited NCIS personnel may be authorized by the Director, NCIS, to carry firearms. These accredited personnel must be appropriately trained and engaged in law enforcement, security, and counterintelligence duties, including:

(1) Law enforcement activities including investigations of espionage, sabotage, and other serious crimes in which DoD programs, personnel or property are the victim; cases where DoD personnel are involved in serious crimes; or where investigations and operations are conducted in hazardous areas or under hazardous circumstances.

(2) Protecting classified information, systems, or equipment.

(3) Protecting the President of the United States, high-ranking Government officials, DoD personnel, or foreign dignitaries.

(4) Protecting DoD assets and personnel.

(5) Guarding prisoners.

b. Per reference (a), the Director, NCIS, may also authorize NCIS personnel who are not engaged in full-time law enforcement, security, or counterintelligence duties to carry Government issued firearms for personal protection within the Continental United States (CONUS). This authorization is contingent upon consideration of all relative circumstances and must be in connection with the employee's professional responsibilities, accomplished within all relative guidelines in this chapter, and authorized as the exception rather than the rule.

c. In situations outside the Continental United States (OCONUS), arming of non-special agent (civilian or military) Navy personnel for personal protection may only be authorized by the Chief of Naval Operations (CNO), Vice Chief of Naval Operations (VCNO), or U.S. Navy Unified Command Component Commanders. In situations OCONUS, arming of non-special agent (civilian or military) Marine Corps personnel for personal protection may only be authorized by the Commandant of the Marine Corps (CMC) or the Assistant Commandant of the Marine Corps (ACMC).

(1) Arming non-special agent NCIS personnel in such circumstances requires identification of credible and specific threats against DoD personnel in the specific region, and the authorization does not extend beyond that specific region. The

probability of the threat in a particular location, the adequacy of support by DoD protective personnel, the adequacy of protection provided by U.S. or host nation authorities, and the effectiveness of other means to avoid personal attacks must be evaluated and deemed insufficient before granting this authority.

(2) If authority to carry a weapon is granted to non-special agent personnel after such consideration, that authority is limited, on a case by case basis, to the specific region in which the personnel are operating and is only for the duration of a specific assignment or threat. This authorization must comply with host nation requirements.

d. The Director, NCIS, delegates his authority to arm non-special agent personnel engaged in law enforcement, security, and counterintelligence duties to the deputy director (DD) and the executive assistant directors (EAD). Non-special agent personnel includes Naval reserve personnel, investigators, or select NCIS operational representatives.

e. Non-special agent personnel will only be armed in the performance of official duties after the following process is completed:

(1) In order for a non-special agent to be authorized to carry a government owned weapon in the performance of official duties, the applicable SAC or deputy assistant director (DAD) must submit a request to carry weapon memorandum justification to 00I for concurrence prior to seeking approval of the request from the DD or the respective EAD. The memorandum must set out the details of the mission essential reasons to arm the employee. Final decision to approve the request is the responsibility of the DD or EAD.

(2) If the requirement to carry a firearm and intermediate weapon is approved for the duration of the non-special agent's employment, then the requirement must be included in the employee's position description. If the requirement to carry is temporary, such as for personal protection, then the authority is limited to six months. If additional time is needed, the authorization process must be repeated prior to completing the first six month period.

f. The SAC or DAD, has the responsibility for recommending to the DD or EAD whether a request to carry a firearm should be approved. Prior to seeking approval from the DD or EAD, the SAC or DAD will seek concurrence for the request to carry a firearm from Code 00I and coordinate with Codes 10A, 10B, and 11B. The SAC or DAD must carefully scrutinize requests and review the need vice approving longstanding office practices authorizing non-special agents to carry weapons. Requests submitted by SACs in OCONUS locations must certify that issuing a weapon to non-special agent personnel complies with host nation requirements.

g. Non-special agent personnel authorized to carry a government issued firearm must meet the following requirements before a firearm is issued:

(1) Approval from the DD or cognizant EAD authority with endorsements from the respective SAC or DAD, and Code 00I concurrence.

(2) Successfully complete a firearms training class, through a Federal Law Enforcement Training Center (FLETC) approved curriculum or successfully complete the NCIS Non-Special Agent Firearms Training Program. The course will include training in judgmental shooting, safety, weapons retention, handcuffing, and escalation of force scenarios. Contact Code 10B upon completing the training course to obtain certificate of training and update the Total Workforce Management Service (TWMS) database.

(3) Compliance with the Lautenberg Amendment.

(4) Complete initial firearm qualification, subsequent qualifications, and quarterly training or, in OCONUS locations, complete annual familiarization consisting of live fire of issued authorized weapons in a manner considered appropriate to the host nation for the purpose of maintaining a level of proficiency.

(5) When armed, the employee possesses the appropriate credentials and OPNAV Form 5512/2 (Rev 6-81), Authorization to Carry Firearms.

h. Required Documentation to Carry Weapons

(1) Special Agents. NCIS special agent credentials document the authority to carry firearms. Issuing credentials authorizing special agents to carry firearms is dependent upon successful completion of the Special Agent Basic Training Program, which includes the required course of instruction for handling firearms.

(a) Reference (a), paragraph 4b, allows the Director, NCIS, or his designee, to authorize special agents to use non-government weapons.

(b) Authority for a special agent to use a non-government weapon must be documented in writing by the SAC or DAD exercising supervisory responsibility for the special agent requesting use of a non-government weapon. For special agents at the SAC/DAD level and higher, this authorization must be signed by the special agent's senior rating official. This document must be maintained in the local firearms files and a copy saved in the employee's official TWMS record, under Uploaded Documents/Weapons Authorizations, by the office exercising supervisory responsibility over the special agent receiving authorization to use a non-government weapon. The written authorization must include the make, model, and serial number of the non-government weapon and specify that only government provided ammunition may be used in the weapon while the individual is performing official duties. The authorization to carry a non-government weapon will be re-certified when the special agent is transferred, or there is a change of weapon carried.

(2) Non-Special Agent Personnel. Authority for all non-special agent personnel to carry a firearm is limited to the actual performance of official duties. The authority to carry firearms is not valid during weekends, after duty hours, and during approved leave periods. Operational conditions may dictate an exception to this policy. The SAC or DAD may authorize, in writing, the carrying of a firearm in an off-duty status within the area of responsibility of the office to which the non-agent is assigned. Non-special agent personnel authorized to carry firearms are limited to the use of government issued weapons only.

(a) The intent of this policy is to limit the times and occasions in which non-special agent personnel will need to be armed.

(b) Non-special agent personnel authorized to carry a firearm on a routine basis will carry credentials issued by Code 11 with appropriate lower card, which reflects the authority to carry firearms while in performance of official duties.

(c) Non-special agent personnel authorized to carry firearms on a temporary or infrequent basis will require written authorization from Code 00I and be issued and carry OPNAV Form 5512/2.

(d) Continuing Authority to Carry Weapons. Written authorization must be revalidated each calendar year for non-special agents to carry firearms. Continuing authorization to carry firearms by all NCIS personnel will be contingent on completing four training sessions and two qualifications each year on each weapon serial number issued or authorized to carry. The first qualification will take place in either the first or second quarter of the fiscal year and the second qualification will take place in either the third or fourth quarter of the same fiscal year. A copy of this written authorization must be maintained in the employee's firearms file maintained by their assigned office. The written authorization must include the make, model, and serial number, of the authorized weapon. The authorization to carry will be re-certified when the non-agent is transferred. This written authorization will be uploaded into the weapons authorization folder located in the TWMS database.

(e) Discontinuing Authority to Carry Weapons. NCIS EADs, ADs, SACs, and DADs are authorized to recover Government issued firearms from NCIS personnel when, in their judgment, retrieval is in the best interest of the service and the safety of all concerned. A verbal report of this recovery must be immediately made to Codes 10A and 00I, or as soon as possible, followed by written notification within two-work days. The Commanding Officer, Office of Military Support (Code 01AM) must be provided a copy of the written notification when the action involves Naval Reserve personnel or any other military personnel assigned to NCIS.

(f) Authorized Firearms. NCIS field components are not authorized to maintain firearms other than those issued by Code 11B or approved personal firearms. NCIS components may not maintain surplus "office asset" weapons or retain weapons to issue

at some future time. All surplus weapons must be returned to Code 11B for maintenance and inspection prior to re-issue.

(1) Standard Service Sidearm. The standard service sidearm of NCIS is the (b)(7)(E) (b)(7)(E) In addition, those personnel deploying in support of military contingency operations will be issued a (b)(7)(E) (b)(7)(E)

(2) Secondary NCIS Weapons

(a) Shotguns. NCIS Code 11B issues the (b)(7)(E) This versatile weapon can (b)(7)(E) (b)(7)(E) Using the (b)(7)(E) ammunition, the shot spread will be approximately (b)(7)(E), hence this ammunition is best used against armed subjects or multiple targets at close ranges where over-penetration of projectiles is a concern. (b)(7)(E) the weapon may be used at greater ranges or against smaller, partially obscured targets.

1. Shotguns will be issued for use only when in the judgment of the SAC, assistant special agent in charge (ASAC), supervisory special agent (SSA) or next in chain of command, it is operationally necessary. Shotguns may also be issued when NCIS special agents are assigned under the operational control of the U.S. Secret Service or other Federal agencies requesting the use of shotguns. Operational conditions may warrant the employment of shotguns due to exigent circumstances. In this case and when seeking approval via the chain of command would hinder response to an exigent circumstance; the qualified operator/handler is waived from seeking approval and may deploy the shotgun for operational use.

2. All special agents must qualify every six months and obtain a passing score on the approved shotgun qualification course, which is detailed in this chapter.

(b)(7)(E)

(b)(7)(E) will be issued for use only when in the judgment of the SAC, ASAC, SSA or next in chain of command, it is operationally necessary, or, when special agents are assigned under the operational control of the U.S. Secret Service or other Federal agency requesting use of (b)(7)(E)

1. When the (b)(7)(E) is used in any operation, only qualified and trained personnel will be authorized to carry and use this weapon.

2. In all operational uses, the standard issue 9mm hollow point load (A260, 147 grain) will be used exclusively with these weapons except as described in

subparagraph 3, below. Requests to use other ammunition types must be submitted to NCIS Code 11B in writing, citing justification for this request, prior to use of any alternate ammunition.

3. In some circumstances these weapons may be deployed to contingency operations with special agent personnel. In these circumstances, the rules of war and combat efficiency preclude the use of hollow point ammunition. In these cases the use of (b)(7)(E) is authorized. In such cases NCIS Code11B and the SAC having cognizance in the area of responsibility must be notified as soon as possible.

(c) (b)(7)(E) NCIS maintains an inventory of selective fire, (b)(7)(E) weapons chambered in (b)(7)(E) North Atlantic Treaty Organization). These weapons can provide relatively long range precision shots on man-sized targets, and can also provide increased volume of fire at close ranges. The (b)(7)(E) generally penetrates cover more than the (b)(7)(E) and can (b)(7)(E) These weapons are useful when long distance shots may be required, and when agents are likely to be facing armed subjects, body armor, or deployed to a contingency operation. Use of these weapons operationally must be authorized by the SAC, ASAC, or SSA and is limited to agency personnel who have been properly trained. The Contingency Response Field Office is the point of contact for issuing these weapons for deployments in support of military missions. All other requests will be directed to NCIS Code 11B.

1. Agents armed with a (b)(7)(E) weapon in CONUS must have completed an advanced training course in the use of the weapon and have a current qualification score on file locally where the weapon is assigned. Special agents must demonstrate a passing score on the approved qualification course, which is detailed in this chapter, every six months to be considered qualified. Unlike shotguns, the sights and stock of (b)(7)(E) weapons can be adjusted for a particular agent, and for that reason each (b)(7)(E) weapon should be designated for sole use by a specific agent in each office.

2. Mechanical modifications to (b)(7)(E) weapons are prohibited. The only aftermarket accessories authorized for use with (b)(7)(E) weapons are a sling and weapon light. If added, qualification should be conducted with these same accessories on the weapon.

(d) (b)(7)(E)

(b)(7)(E)

suited for NCIS missions requiring a lightweight, compact, highly concealable, select fire weapon system. Use of these weapons operationally must be authorized by the SAC, ASAC, or SSA and is limited to agency personnel who have been properly trained. Operation and training for the (b)(7)(E) is similar to that of the (b)(7)(E) providing

a training platform for the (b)(7)(E) hat can be utilized at most CONUS locations that may have ammo or range restrictions for rifles.

(e) (b)(7)(E) is maintained for use by agency personnel requiring weapons compatibility when assigned with military forces in a deployed status; these weapons are controlled by NCIS Code 11B. The (b)(7)(E) pistols are presently issued to CONUS offices for training purposes only and may not be issued or used operationally without authority from NCIS SACs or DADs. Personnel will qualify with the (b)(7)(E) on the standard NCIS training and qualification course prior to being issued the firearm.

(f) Special Purpose Weapons. In specific instances, such as long-term undercover assignments, a weapon, not readily identifiable with law enforcement, may be required for operational use. The requesting office will coordinate with NCIS Code 11B and an appropriate weapon will be identified and procured. This weapon will be receipted for and, upon completion of the specific operation, will be surrendered to NCIS Code 11B for disposition.

(g) Personal Weapons. Special agents are authorized and can carry both government issued NCIS weapons and approved personally owned weapons at the same time when authorized to carry a weapon. Personnel must qualify with authorized weapons twice per year. The first qualification will take place in either the first or second quarter of the fiscal year and the second qualification will take place in either the third or fourth quarter of the same fiscal year. Prior to transferring to an OCONUS location, the transferring individual is responsible to consult with the receiving field office relative to weapon or caliber restrictions imposed by the host country, the Status of Forces Agreement (SOFA), or State Department in the field office area of responsibility. Personal weapons shall not be carried into contingency operations. Non-special agent personnel authorized to carry firearms are limited to the use of government issued weapons only.

(1) Pistols and revolvers from the following manufacturers are acceptable for special agent carry provided all other criteria are met:

(b)(7)(E)

(b)(7)(E)

(2) Personal weapons must not be modified for competition. Specifically excluded are pistols with (b)(7)(E) or other modifications designed for competition. In addition, all safety devices must remain functional.

(3) Personally owned (b)(7)(E) must meet the following criteria:

(a) Pistols must be chambered for (b)(7)(E) (b)(7)(E)

(b) Have a minimum capacity of (b)(7)(E)

(b)(7)(E)

(d) If the weapon and/or operator are found to be unsafe, the weapon difficult for the operator to utilize on the range, or the weapon found to be unreliable on the range; an NCIS firearms instructor may deem the weapon inappropriate for carry by the operator. The NCIS firearms instructor will make the decision regarding the suitability of a weapon based on the operator's ability to properly and safely handle the weapon.

(e) Government owned and issued (b)(7)(E) is the only ammunition allowed for duty carry.

(4) In addition to the above (b)(7)(E) personnel authorized to carry a weapon may also carry personally owned (b)(7)(E) meeting the following specifications:

(b)(7)(E)

(b) Revolvers shall be (b)(7)(E)

(b)(7)(E)

(b)(7)(E)

(f) If the weapon or operator is found to be unsafe, the weapon difficult for the operator to utilize on the range, or the weapon found to be unreliable on the range; an NCIS firearms instructor may deem the weapon inappropriate for carry by the operator. The NCIS firearms instructor will make the decision regarding the suitability of a weapon based on the operator's ability to properly and safely handle the weapon.

(g) Government owned and issued (b)(7)(E) is the only ammunition allowed for duty carry.

(5) With the exception of ammunition, which must be Government supplied, all accessories required for the weapon are the responsibility of the individual owner-operator. While some personally owned weapons will properly fit the agency provided leather gear, NCIS will not otherwise provide holsters, magazine carriers or maintenance support for personal weapons. Maintenance and repair of personal weapons is the responsibility of the individual owner-operator.

(6) Following successful qualification with a personally owned weapon, a letter from the SAC or DAD will document the approval of all personal weapons. The letter must describe the weapon by manufacturer, model name or number and serial number and specify that only government issued ammunition may be used in the weapon while the individual is performing official duties. The letter will be maintained in the personnel and firearms file, with a copy scanned into the employee's official TWMS record under Uploaded Documents/Weapons Authorizations. The office with supervisory responsibility over the special agent receiving authorization to use personal weapons is responsible for ensuring a copy of the document is saved in the employee's official TWMS record, under Uploaded Documents/Weapons Authorizations. The authorization to carry personal weapons remains in effect for the duration of an agent's assignment. The personal weapons carry authorization must be renewed upon transfer to another duty location or at the request of the field office SAC or DAD.

34-9. Proper Carry of Firearms

a. Special Agents. Special agents will be armed when in a duty status in the 50 United States and its territories or possessions:

(1) NCIS special agents are required to carry firearms when any of the following conditions apply and regardless of duty status. While:

(a) Traveling (to include commercial air) on official orders, unless specifically directed otherwise.

(b) Traveling between their residence and the NCIS office.

(c) Serving as a duty agent or alternate duty agent.

(d) Within the jurisdictional area of the special agents' assigned duty station and there is some reasonable expectation that they may be called upon to return to duty status.

(2) Exceptions. Exceptions are limited to situations where wearing of firearms by sworn law enforcement personnel would be inappropriate or constitute a safety hazard. Examples include court appearance, when in an exclusion area, or when traveling to or in OCONUS locations where host nation laws and the SOFA prohibit transport and/or carrying of firearms, ammunition, and/or intermediate weapons.

b. Non-Special Agent Personnel. Non-special agent personnel, having written authorization, can be armed when in an applicable duty status in the 50 United States and its territories or possessions.

(1) If mission requirements dictated that non-special agent personnel be armed while in a temporary additional duty (TAD) status, authorization must be established by the SAC or DAD. This authorization is limited to the area of the TAD mission only for the portion of the TAD during which carrying the firearm is required. Additionally, non-special agent personnel, unless assigned to PSO missions, are not authorized to fly armed.

(2) Non-special agent personnel are not authorized to carry firearms in an off-duty status. Operational conditions may dictate an exception to this policy. The SAC or DAD may authorize, in writing, the carrying of a firearm in an off-duty status within the area of responsibility of the office to which the non-agent is assigned.

a. Carrying firearms or an authorized intermediate weapon may be inappropriate in some situations. Special agents and non-special personnel authorized to carry weapons are expected to exercise common sense and good judgment when assessing local conditions and the decision to carry a firearm. Everyone should avoid unnecessary reference to the fact they carry a firearm on their person.

b. In foreign countries, all NCIS personnel will carry firearms only under conditions specified by the Combatant Commander, and coordinated with host foreign authorities in accordance with SOFA requirements.

34-10. Physical Method of Carrying Firearms. Code 11B issues firearms, magazines, holsters, handcuffs, extendible baton, magazine carriers, and speed loaders as appropriate to qualified NCIS personnel.

a. Sidearms should be worn with the holster issued by NCIS. However, agents may use personal holsters under the following conditions: Personal holsters must be safe, be in good operating condition, adequately conceal the weapon, be suitable to the agent's physique, and comply with all NCIS guidelines. In order to carry personally owned holsters, the special agent must qualify with the holster. The following prohibitions apply:

(1) Personal holsters leaving the trigger guard exposed or allowing for the insertion of a finger into the trigger guard while holstered.

(2) Purses, briefcases, or carrying cases which do not fix the weapon firmly onto the agent's body.

b. The SAC, or DAD may authorize, in writing, the use of any holster or other method of carrying firearms which, in the SACs or DADs judgment, is suitable or necessary.

c. When armed, the special agent will also carry a complete ammunition reload (a full magazine or speed loader) and handcuffs or restraints. The NCIS authorized intermediate weapon should be carried; however, in cases where operational considerations dictate otherwise, handcuffs and the baton may be dispensed.

34-11. Using Firearms and Use of Force During Duty. The proper use of force is a critical concern in contemporary law enforcement. NCIS special agents, and non-agent personnel authorized to carry firearms, may be confronted with situations requiring them to make split second decisions, some which may have severe and life threatening consequences for the agent, the offender, and citizens served. Training provides the agent with the knowledge and skills needed in the critical decision making process. Perhaps no issue can impact the personal and professional career of a law enforcement officer more than a lawsuit alleging excessive use of force. NCIS has adopted the use of force guidance set forth by the FLETC. This guidance is provided to all special agents attending the Criminal Investigators Training Program (CITP) at FLETC. Although the term "special agent" is used, the policy applies to all NCIS employees and reserve personnel authorized to carry firearms. Reference (d) specifies the conditions in which deadly force may be used. NCIS specific use of force policy, in addition to reference (d) requirements, are included in this section.

a. NCIS Use of Force Policy. Special agents or non-agents authorized to carry a firearm may use deadly force only when necessary, that is, when the special agent or non-agent has a reasonable belief that the subject of such force poses an imminent danger of death or serious physical injury to the special agent, non-agent or another person. The standard that will be used to measure the agent or non-agent's actions will be that of

"objective reasonableness." The shooter's use of deadly force will be viewed in light of the facts and circumstances confronting him or her at the time of the incident.

(1) Fleeing Subjects. Deadly force may not be used solely to prevent the escape of a fleeing subject. However, deadly force is authorized when a special agent or non-agent has probable cause to believe that the subject has committed a crime that involved the infliction or threatened infliction of serious physical harm, that deadly force is necessary to prevent the subject's escape, and the fleeing subject poses an imminent danger of death or serious bodily harm to law enforcement and/or security personnel or another person.

(2) Disabling Vehicles. Firearms may not be fired solely to disable moving vehicles, vessels, aircraft, and other conveyances.

(3) Verbal Warnings Prior to Use of Deadly Force. If feasible, and if to do so would not increase the danger to the special agent, non-agent or others, a warning to submit to the authority of the special agent or non-agent shall be given prior to the use of deadly force.

(4) Warning Shots. Warning shots are prohibited.

(5) Military Deployed Status. The NCIS use of force policy applies worldwide, except where competent authority, such as unified combatant commanders, modifies such rules for non-combatants.

b. When Deadly Force is Not Authorized. NCIS special agents or non-agents must use alternative methods and tactics for handling resisting subjects who do not pose an imminent danger of death or serious physical injury to the special agent, non-agent, or another person. NCIS authorizes the use of the extendible baton as the striking instrument and the sole intermediate weapon. Using the extendible baton must be objectively reasonable based upon the totality of the circumstances known to the special agent or non-agent at the time of the incident. NCIS does not authorize using other intermediate weapons, including Oleoresin Capsicum (OC) spray or the use of any control weapons.

c. Drawing Your Firearm. NCIS special agents or non-agents may draw their weapon when there is reason to believe they might need it to protect their life or that of another. Premature drawing of a weapon creates unnecessary anxiety for the suspect and innocent bystanders and could result in accidental discharge. The decision to draw and exhibit a weapon must be based on common sense and a reasonable perception that the situation could escalate to the need for deadly force. When a firearm is drawn to effect an apprehension or arrest, said action will be thoroughly documented in the investigative action (IA) detailing the action.

d. Discharge of a Firearm. A firearm discharge, other than during authorized training, or any instance of mishandling of firearms by NCIS personnel, will be reported immediately through their next level supervisor to Code 00I. The preliminary report will

indicate the type and reason for the discharge (e.g., accidental, self-defense, military operation) as well as contain sufficient detail for a determination to be made as to the need for additional inquiry by Code 00I. Military operation reports, unit situation reports, and after-action reports do not satisfy this NCIS reporting requirement. The purpose of the initial report is to enhance situational awareness of the NCIS executive staff and permit assessment of the danger of a particular area, operation, mission or deployment; initiation of appropriate contingency scenarios; and preparation for inquiries generated by outside interests, to include possible next-of-kin contacts.

e. Loss or Theft of Firearm(s). Immediately report the loss or theft of firearms (government and personal/non-government firearm authorized for official use) to the next level supervisor. The supervisor is responsible to notify Code 00I regarding the loss or theft of firearms (government and non-government). If the firearm is government issued, the supervisor is also responsible to notify Code 11B.

34-12. Flying Armed On Commercial Aircraft. In accordance with references (f) and (g), it is a federal crime for anyone aboard an aircraft operated by a U.S. licensed carrier in air transportation to have on or about his or her person, a concealed deadly or dangerous weapon. Excluded are law enforcement officers and other persons as may be authorized by the Department of Transportation (DOT), Transportation Security Administration (TSA). TSA regulations and reference (h) identify those persons who may carry weapons on-board civilian aircraft as sworn law enforcement officers of the Federal, state, and local governments who are authorized to enforce criminal or immigration law, as well as those persons conducting PSO mission.

a. Reference (a) provides guidance for DON personnel transporting and carrying firearms onboard an aircraft.

b. The DOT and TSA have prescribed additional procedures for the carrying of a firearm aboard an aircraft. Those procedures are set forth in the training guidance prepared by TSA and provided to field office trainers by Code 10B. Prior to carrying a weapon aboard a commercial aircraft, all special agents or non-special agent personnel authorized to carry firearms in support of PSO missions are required to complete training complying with TSA and Code 10B assigned firearms instructors.

c. SECNAV instruction and TSA policy provides that a special agent may have on or about their person a concealed firearm while a passenger on any aircraft operated by a U.S. licensed aircraft carrier operating in CONUS. Carrying a firearm is authorized in a duty or non-duty status provided the firearm is properly declared and airline required forms are properly completed. The pilot in charge of the commercial aircraft is the in-flight security coordinator and makes the decision allowing the firearm aboard the aircraft.

d. TSA regulations allow sworn accredited Federal law enforcement officers, such as a special agent, to carry a firearm on their person while a passenger on an aircraft, provided:

(1) It is operationally necessary and the special agent is authorized by the employing agency [NCIS] to carry the firearm. In the case of special agents, and as noted above, this applies to travel on official orders or personal travel.

(2) The special agent is using commercial air in CONUS.

(3) Prior to departure (one hour, or in an emergency as soon as practicable, before departure), the NCIS special agent will discreetly contact a responsible representative of the airline and display their credentials and advise of the need to remain armed during the flight and:

(a) Complete a TSA approved form and be prepared to present a second picture identification. The special agent is also required to provide an agency code, or Unique Federal Agency Number (UFAN) to verify status as a Federal agent. The UFAN is a law enforcement sensitive code, which is periodically changed, and may be obtained from the NCIS Multiple Threat Alert Center (MTAC).

(b) The commercial airline representative is obliged to inform the captain of the aircraft of the presence and seat location of the armed special agent. If the aircraft commander objects to the carrying of the firearm, the special agent should use discretion in addressing the issue. Conflicts that cannot be amicably resolved must be directed to the station manager or designated airline ground security advisor or TSA representative. TSA authorizes Federal agents to fly armed when traveling in other than an official status and such a practice is not prohibited by this policy. NCIS special agents are required to notify their immediate supervisor as soon as possible when problems are encountered.

(c) Special agents may not consume alcoholic beverages while travelling armed on a commercial aircraft.

34-13. Intermediate Weapons

a. Intermediate weapons are categorized into three groups: impact weapons, control weapons, and Oleoresin Capsicum (OC) spray. NCIS authorizes use of the extendible baton as the impact weapon and the sole intermediate weapon; no other intermediate weapons or control weapons are approved. OC spray is no longer issued or authorized for use by NCIS employees. Some OCONUS jurisdictions may prohibit the possession or use of extendible batons, and it is the responsibility of the SAC OCONUS location to determine if SOFA or local laws prohibit possession and use of batons.

b. The (b)(7)(E) model extendible baton has been authorized as the intermediate weapon for NCIS personnel who have trained and qualified with the baton. No other types of baton are authorized, nor are any modifications to the NCIS issued extendible baton, with the exceptions of the NCIS issued grip cap, or leverage cap.

c. The extendible baton will be issued to all NCIS personnel who perform a law enforcement function and have completed required training. NCIS special agents completing the FLETC CITP have received required baton training; all other personnel will obtain training at their respective field office or code from trainers who have completed the Law Enforcement Control Tactics Instructor Training Program (LECTITP). Additionally, annual baton training administered by a certified instructor is required. The lesson plan for the baton can be found on the NCIS Code 10B Lighthouse site under "In-service Training."

d. All personnel who have been trained in the use of the extendible baton should carry this intermediate weapon as part of their routine issued equipment (sidearm and handcuffs) during on-duty status when practical. This practice ensures personnel have every tool necessary to respond to threats using a full spectrum of force. In situations where concealing the baton is not practical or legal, such as undercover operations or while traveling OCONUS, personnel are excused from carrying the baton.

e. Guidelines for Use of the Extendible Baton. A special agent may use deadly force only when they have a reasonable belief a subject poses an imminent danger of death or serious bodily injury to the agent or to another person. The extendible baton may be used in circumstances where deadly force is not justified, but require a use of force to bring a non-compliant or assaultive subject under control.

(1) Use of excessive force beyond that necessary to effect a lawful arrest or apprehension is prohibited by Federal and state statutes, and violations of these statutes can carry both civil and criminal penalties.

(2) Extendible baton strikes should be delivered to large muscle groups of the body or the limbs of an attacker whenever possible. Avoid intentional strikes to the head, heart, spine, and groin area unless faced with conditions which merit the use of deadly force.

f. Post-Incident Procedures. NCIS personnel must immediately report the use of an extendible baton. Exceptions to this reporting requirement are the use of an extendible baton during training, practice, or when the weapon is used as a searching aid. Use of an extendible baton, except as described above, requires reporting of the incident as follows:

(1) Special Agent. Immediately report the incident to the SAC or DAD or immediate supervisor, and if appropriate, local law enforcement authorities, and a written detailed report will be provided to his/her supervisor.

(2) SAC and DAD. The SAC and DAD must immediately report facts and circumstances of the incident to the Code 00I, with an information copy to NCIS Code 10B.

g. Responsibility at the Scene. All personnel are required to exhibit sound judgment after the use of an impact weapon. At a minimum, the following shall be completed:

(1) Determine the physical condition of any injured person and render aid when appropriate.

(2) If necessary, request emergency medical aid and notify local law enforcement authorities of the incident and location.

(3) Immediately notify their supervisor and follow procedures for handling critical incidents, if appropriate.

(4) Upon formal request by a competent authority having jurisdictional responsibility, involved NCIS personnel will prepare a detailed report of the incident to be approved by their SAC or DAD. Upon request, involved personnel will be afforded reasonable time to consult with their supervisor or personal legal counsel prior to preparing the report.

(5) Involved personnel will not release any information concerning the incident to individuals outside of NCIS, other than to his/her personal legal counsel, without the approval of their immediate supervisor.

34-14. Legal and Administrative Considerations. Personnel involved in a deadly force incident where a suspect, bystander or special agent or law enforcement officer is killed or critically or permanently injured, shall, at the discretion of the Director, NCIS, be placed on administrative leave following report of the incident. A person placed on administrative leave does not imply improper actions. Administrative leave does not result in loss of pay or benefits. Administrative leave will remain in effect through the completion of the investigation of the incident. Persons placed on administrative leave are subject to recall to duty at any time, and will remain available for interviews, statements, etc. The only exception will be when the employee is seriously injured or under medical care and competent medical authority recommends against such interviews. Upon returning to duty, the personnel may be assigned limited or other non-investigative (administrative) duty for the appropriate amount of time recommended by the employee's supervisory chain of command and/or medical personnel.

a. Documentation of Shooting Incidents. Shooting incidents by an NCIS employee must be reported, documented, and investigated. The circumstances surrounding a shooting incident will dictate the nature of the report submitted and the subsequent level of investigation and review. Code 00I will make the decision to conduct a shooting incident inquiry. Prompt and appropriate measures must be taken to ensure that NCIS shooting inquiries are thorough, factual, and objective. Reference (i) provides additional guidance pertaining to shooting incidents.

b. Accidental Discharges. Whenever a special agent accidentally discharges their weapon in a tactical or operational setting, regardless if anyone is injured or killed, it is considered a major incident and applicable procedures from reference (i), shall be followed.

c. Weapon Discharge in Contingency Operations. When NCIS personnel discharge a weapon in designated hostile fire areas, contingency operations, or during military deployments governed by rules of engagement as defined by the combatant commander, a determination as to appropriate immediate action to be taken, to include the decision for the incident employee to maintain custody of their weapon(s), will be made by the on-scene NCIS supervisor or senior military or mission commander based on the tactical situation and threat. As soon as a tactically stable condition exists, the incident employee will comply with notification and documentation requirements as directed above.

d. Additional Considerations Involving Firearms. NCIS restrictions on the use of firearms shall not apply during contingency operations or when deployed to designated hostile fire areas when rules of engagement for personnel deployed to those areas are implemented by competent authority, such as unified combatant commanders.

e. Shooting Incident Inquiries. During investigations of shooting incidents, the investigative needs of NCIS or other law enforcement agencies will take precedence. Reference (i) contains additional detailed guidance in handling discharges of firearms where injury or death occurs. Specifically, the section entitled, "Incident Scene Management Roles" addresses the guidelines and specific duties assigned. Code 00I shall be responsible for investigative determinations regarding any shooting incident. The initial report of a shooting occurrence is intended to promptly document the incident and involve Code 00I and executive staff in appropriate oversight of decision making and investigative processes. The initial report must contain sufficient information to allow senior managers to make informed judgments regarding the necessity, type, and depth of subsequent inquiries, which may include administrative investigations under the authority of reference (j). The circumstances surrounding shooting incidents will dictate the complexity and type of investigation to be conducted, the nature of reports submitted, and the level of review to which the incident is subjected. Field office and NCIS Headquarters senior managers will ensure that initial relevant details regarding the incident are documented and expeditiously provided to Code 00I and appropriate executive staff to support the inquiry and review process.

(1) Shooting incident inquiries will be conducted with due regard for the physical, mental, and emotional well-being of the employees involved, their families, co-workers, victims, and witnesses. The purpose of the reporting, investigative, and review process is to provide senior management with a factual basis for evaluating operational activities; assessing the reasonableness of the conduct; and determining the effectiveness of training, planning, judgment and other factors that may compromise operations or the safety of employees.

(2) Additional policy concerning the conduct of post-shooting incident reviews, to include guidance pertaining to a review board process, continues to be developed and will be defined in a forthcoming revision to reference (i).

34-15. Firearms Training, Qualification, and Safety. Supervisors at NCIS field offices and headquarters departments must ensure NCIS employees who carry firearms comply with this firearms training, qualification and safety policy. Firearms qualification (meeting or exceeding a specified minimum score) is required with the NCIS authorized or approved handgun and shotgun. Selected special agents must maintain qualification on (b)(7)(E) weapons in order to be deemed qualified as handlers. Armed personnel assigned a NCIS issued weapon and special agents approved to carry personally owned handguns, must qualify with these weapons prior to carrying either and/or all weapons. Qualification with a similar type weapon is acceptable in only very rare circumstances such as overseas venues or while on deployment when qualification opportunities are limited. If armed personnel are not in possession of a NCIS issued weapon and are approved to carry a personally owned handgun, they only have to qualify on that personally owned weapon, but are not authorized to carry a NCIS issued weapon. Prior to the qualification sessions, firearm instructors will brief all those in attendance on range safety procedures and use of force policy. The qualification courses of fire for (b)(7)(E) are derived from the most current FLETC lesson plans and can be found on the NCIS Lighthouse website under Code 10B "Firearms Instructors/Use of Force." Initial training requirements for armed personnel are as follows:

a. Special Agents. All newly hired NCIS special agents will attend the CITP, at FLETC, Glynco, Georgia, where they will be trained in the appropriate use of deadly force. Training will be conducted with the weapon they will be issued upon graduation, so the special agent will be completely familiar with the issued weapon. Special agents hired from other Federal agencies will undergo initial firearms training with their issued weapon in the field or while attending the Special Agent Basic Training Program (SABT) at FLETC.

b. Non-Agent Personnel. The entire process of arming non-agents shall be under the direction of and monitored by the NCIS Code 00I. All required training must be documented in TWMS.

(1) All non-special agent personnel authorized to carry a government firearm must successfully complete a firearms training class, through a FLETC approved curriculum or successfully complete the NCIS Non-Special Agent Firearms Training Program. The NCIS Non-Special Agent Firearms Training Program is located on the NCIS Lighthouse website and is at least 40 hours in length and concentrates on marksmanship, essential weapons handling skills, and mind set training for deadly force encounters. The course shall also contain lecture based use of force training tailored to suit the purpose for which the non-agent is authorized to be armed; the NCIS Training Academy, Code 10B is available for consultation if needed. The course of instruction shall culminate in a standard NCIS qualification course of fire, and all shooters shall meet the minimum 240/300 (80 percent) score, and shall be further tested by a written multiple choice test provided by Code 10B. Following completion of this initial training, Code 10B will provide certificates of completion and document the training in the TWMS. Having qualified on their weapon, non-special agent personnel authorized to carry a government

firearm must continue to qualify on their weapons in accordance with section 13-15(c) below.

(2) Active Duty Reserves. Active duty and military reserve members attached to NCIS but not otherwise addressed by this chapter shall meet the requirements of the applicable service component relative to that services weapons qualification standards. In addition, all training and qualifications shall be conducted by the applicable service component and documented in the members' service record.

(3) 1810 Investigators Used in a Law Enforcement Capacity. Personnel assigned as GS 1810 Investigators shall meet the same training and in-service qualifications as the special agent. Initial training shall include:

(a) NCIS Non-Special Agent Firearms Training Program.

(b) Use of Force training as taught in FLETC CITP.

(c) Control tactics as taught to special agents.

(4) Active Duty Military Members Assigned to PSO Duty. Personnel assigned to the PSO mission are authorized to carry the government owned weapon only while actively participating in a PSO mission or function. Use of force training for these personnel shall stress their obligations while protecting a principal and that while "off duty" or not engaged in a PSO mission, they have no duty or authorization to act. Active duty or reserve military personnel assigned to NCIS, who perform PSO duties shall meet the minimum qualifications of the respective service component and in addition shall meet the following NCIS training requirements prior to conducting PSO missions:

(a) Basic weapons handling course. NCIS Non-Special Agent Firearms Training Course.

(b) Use of force (tailored to PSO mission, i.e. protection of principle only).

(c) Control tactics (tailored to PSO mission).

(5) Civilians Authorized to Carry Weapons for High Risk Missions Only. NCIS personnel authorized to carry a Government weapon while assigned to High Risk Missions shall meet the following initial training requirements:

(a) NCIS Non-Special Agent Firearms Training Course.

(b) Use of force and rules of engagement training as required by the applicable Theater Commander, State Department or SOFA requirements depending on location.

(6) Civilians Authorized to Carry Weapons for Providing Security to DoD and U.S. Navy Property. NCIS personnel authorized to carry a government weapon solely to provide security to property shall meet the following initial requirements:

(a) NCIS Non-Special Agent Firearms Training Course.

(b) Use of Force training tailored to mission or specific responsibility, i.e, self-defense or defense of property (e.g. automatic weapons, munitions evidence, etc.

c. Qualification Responsibilities for Personnel Assigned in the United States

(1) Special agents and non-agent personnel authorized to carry weapons for law enforcement purposes will attend quarterly mandatory training sessions of approximately four hours in length, to include use of force in-service training provided on-line, and will qualify with each NCIS issued handgun and approved personal handgun twice per fiscal year. The first qualification will take place in either the first or second quarter of the fiscal year and the second qualification will take place in either the third or fourth quarter of the same fiscal year.

(2) Range sessions will be conducted with a mix of training designed to maintain proficiency and competency with the weapons, as well as a qualification course of fire conducted subsequent to training. Range sessions will consist of an appropriate mixture of drills found on the NCIS Lighthouse website under Code 10B "Firearms Instructors/Use of Force." Designated personnel will also qualify and familiarize with department issued shoulder weapons as outlined below. With the exception of firearms instructors (FI), personnel having both issued and personal weapons are required to qualify with each weapon twice per fiscal year to maintain authorization to carry each weapon.

(3) Upon completion of required firearms training and qualification, TWMS records will be updated by the respective Field Training Coordinator (FTC) or Headquarters Training Coordinator (HTC) upon receipt of the official range roster from the coordinating FI. Range rosters shall be verified by the FTC/HTC to ensure the make/model/serial numbers used for qualification by each person match the weapons information within TWMS. The NCIS Handgun Training report within TWMS can be accessed and used by FTC/HTCs for this purpose. All NCIS personnel issued a government handgun and/or who have current authorization to carry personally owned weapon(s), are required to input and maintain accurate weapons inventory data within their TWMS Self-Service record.

(4) The SAC of each CONUS field office or DAD for each headquarters code shall ensure that each NCIS special agent and non-agent under their command is afforded the opportunity to attend firearms sessions as necessary to meet these qualification requirements. If the shooter fails to attain a passing qualification score of 80 percent (240/300), they will be afforded two additional attempts to qualify during that qualification period and given time with a firearms instructor for remedial instruction.

(5) Should the shooter fail to attend mandatory range sessions or fail to qualify, the individual's SAC or DAD will notify the employee in writing of their non-compliance with policy and direct them to take appropriate actions to qualify within the next 45 days. During this period, personnel will be afforded the opportunity for additional one-on-one training with a firearms instructor. The SAC or DAD will forward a memorandum to the appropriate EAD or AD citing the employee's reasons for non-compliance with a copy to NCIS Code 00I. Employees failing to qualify within the 45 day "remediation" period will be notified of their continued non-compliance and a copy of this notification will be forwarded to Code 00I for action.

(6) Personnel are required to perform at the 80 percent level (240 of a possible 300 points) in order to attain a passing score on the qualification course of fire using the Trans-Star IV targets. Numerical scores will not be reported on the qualification score sheets. Shooters who score 240 or higher will be recorded as "pass" and those scoring less than 240 points will be recorded as "fail." Firearms qualifications records will be retained at the field office level for a period of two years. These records should contain the following information:

(a) Employee's name.

(b) Firearm Instructor's (FI) name.

(c) Last four (4) digits of the social security number.

(d) Description the of weapon – personal and/or government; i.e., (b)(7)(E) etc.

(e) Pass or fail (no numerical score).

(f) Date of qualification.

(7) A minimum of a single four-hour session of mandatory training will be required in those quarters where qualification did not take place and will consist of drills selected by the local firearms coordinator from the approved list on the NCIS Lighthouse website under Code 10B "Firearms Instructors/Use of Force." Special agents must complete a qualification course of fire with the pistol following the mandatory training session in those quarters where qualification takes place and achieve a passing score of 80 percent (240/300). Those not participating in the training will not be permitted to qualify, and those not firing a passing score must be remediated as outlined above in section (2).

(8) One quarter of mandatory training will consist of drills and force-on-force scenarios using designated (b)(7)(E) weapons modified to fire Non-Lethal Training Ammunition (NLTA), commonly referred to as (b)(7)(E) and approved protective equipment. Training will be accomplished in one four-hour training session and only be conducted by firearm instructors trained in NLTA procedures at an approved FLETC course and utilizing issued weapons and ammunition. Trainers will use any drill

selected from an approved list on the NCIS Code 10B Lighthouse website by the NLTA instructor. Until such time as each field office has acquired NLTA equipment, blue guns, and a trained instructor, the quarterly mandatory training may consist of any drill from the approved list.

(9) One quarter of mandatory training will consist of basic pistol drills from the approved list and a shotgun qualification course using the (b)(7)(E) shotgun and a combination of (b)(7)(E) All special agents will fire the shotgun qualification course. The Code 10B Lighthouse Site contains additional information on the shotgun qualification course.

(10) Pregnant special agents and pregnant non-agent personnel are exempt from firearms qualifications during their pregnancy and for a period of up to 6-months afterward, with authorization from a SAC or DAD. They are permitted to carry their weapons, providing they have qualified during the period preceding their pregnancy. This policy represents the minimum standards and does not limit a SAC or DAD from scheduling and reporting qualifications or proficiency training that goes beyond the specified minimum requirements.

d. Overseas Assignment Qualification Responsibilities. NCIS special agents assigned as permanent change of station (PCS) personnel or on TAD assignment overseas, who are qualified at the time of departure, shall be considered to remain qualified while outside the U.S. as long as the tour does not exceed 5 years. At a minimum, agents shall conduct familiarization firing of the qualification course of fire with each NCIS issued handgun, approved personal handgun, and shotgun once every fiscal year while overseas. Records of these shoots will be recorded on score sheets as "Fam" and input into TWMS by the local office using the assigned course code identification on the In-Service Training Matrix as "Overseas Handgun Familiarization." With the exception of FIs, personnel having both issued and personal weapons are required to complete familiarization firing with each weapon once per year to maintain authorization to carry each weapon. Upon completion of required familiarization firing, TWMS records will be updated by the respective FTC or HTC upon receipt of the official range roster from the coordinating FI. Range rosters shall be verified by the FTC/HTC to ensure the make/model/serial numbers used for familiarization firing by each person match the weapons information within TWMS. The NCIS Handgun Training report within TWMS can be accessed and used by FTC/HTCs for this purpose. All NCIS personnel issued a government handgun and/or who have current authorization to carry personally owned weapon(s), are required to input and maintain accurate weapons inventory data within their TWMS Self-Service record. All special agents returning from overseas shall qualify by the end of the next quarter upon return to the U.S. and OCONUS special agents who extend beyond the 5-year point will be required to qualify at or before the 5-year point.

e. Shoulder Fired Weapons

(1) Shotgun. To be considered an operator or handler for the shotgun, the agent must have successfully completed the shotgun qualification course of fire.

Operators/handlers must qualify with the shotgun twice per fiscal year, as required for the handgun, in quarters one or two and again in quarters three or four, with a minimum score of 80 percent (b)(7)(E) requires 64 hits and not more than 16 misses, using (b)(7)(E) requires 96 hits and not more than 24 misses (b)(7)(E) (b)(7)(E) Shotgun operator/handler status lapses for any agent who fails to qualify twice per fiscal year. In order to re-instate shotgun operator/handler status, the operator/handler must demonstrate their proficiency with the weapon by again shooting a qualifying score. The Code 10B Lighthouse Site contains additional information on the shotgun qualification course. Those not attaining a score of 80 percent will be recorded as "Familiarized" or "Fam" on the qualification record and will not be permitted to carry a shotgun operationally. Those who have attained a score of 80 percent or better will be designated as "Handler" or "H" on the qualification sheet, and may be permitted to carry a shotgun on NCIS operations.

(2 (b)(7)(E) To be considered an operator or handler for the (b)(7)(E) the agent must have gone through the (b)(7)(E) or Automatic Weapons Operator Course (AWOC). To be considered an operator or handler for the (b)(7)(E) the agent must have gone through the NCIS Submachine Gun Operator or Automatic Weapons Operator Course (AWOC). Operators and handlers must qualify with the weapon twice per fiscal year as required for the handgun, in quarters one or two and again in quarters three or four, with a minimum score of 80 percent (40 out of 50 hits on target). Submachine gun certification lapses for any agent who fails to qualify twice per fiscal year. In order to re-instate the submachine gun certification, the operator/handler must demonstrate their proficiency with the weapon by shooting a qualifying score and conducting both day and reduced light standards with the (b)(7)(E) In field offices where there is no qualified Submachine Gun Instructor, any FLETC Firearms Instructor Training Program (FITP) qualified instructor may call the course of fire for operators/handlers for qualification.

(3 (b)(7)(E) It is recommended each special agent and non-agent deploying to a high risk environment receive training on the (b)(7)(E) similar to that provided in the High Risk Operations Training Program (HROTP). In the case of multiple deployments, the shooter should receive refresher training on the weapons system prior to each re-deployment. To be designated a (b)(7)(E) weapons handler within the U.S., NCIS special agents must complete the initial 40-hour Automatic Weapons Operator Course (AWOC) and qualify with the assigned weapon twice per fiscal year as required for the handgun, in quarters one or two and again in quarters three or four, with a minimum score of 80 percent (40 out of 50 hits on target). As with the (b)(7)(E) the qualification standard is 80 percent. Due to changes in course content and record keeping, the HROTP and other pre-deployment training do not always meet the threshold to handle a (b)(7)(E) weapon in the U.S.; therefore, Code 10B should be consulted prior to assigning weapon to any agent who has not successfully completed AWOC.

f. Firearms Instructor Qualifications

(1) NCIS special agents or other personnel must successfully complete the FLETC FITP before they are qualified to conduct firearms training and qualifications for the handgun and shotgun. Once the FLETC training has been completed, the special agent or other personnel will remain a qualified instructor until they leave the position, provided they remain active. Firearms instructors should coordinate refresher training with Code 10B approximately 5 years after attending the basic FITP course. Though not mandatory, the refresher training will help instructors maintain their proficiencies and instructional techniques, as well as keep them abreast of current techniques and trends in firearms instruction.

(2) Submachine Gun Instructor Qualifications. The NCIS special agent or other personnel must successfully complete the (b)(7)(E) Instructor Training Program course or the Automatic Weapons Instructor Training Program (AWITP) before they are qualified to instruct employees in the use of the (b)(7)(E) or other automatic weapons. The FITP and the Submachine Gun Operator course or Automatic Weapons Handler Course are pre-requisites to enrollment in the instructor course. Non-agent instructors must be supervised by a special agent instructor in order to train and qualify special agents on the weapon system. Submachine Gun Instructors must qualify twice per year at the 85 percent level (43 out of 50 hits on target).

(3) (b)(7)(E) Instructor Qualifications. The NCIS special agent or other personnel must successfully complete the 40-hour AWITP before they are qualified to instruct agents in the use of the (b)(7)(E) weapons system for CONUS use. The FITP and Submachine Gun Operator Course or Automatic Weapons Handler Course are pre-requisites to enroll in AWITP. Due to differences in course content, Submachine Gun Instructors must be retrained as AWITP instructors before training agents in the use of the (b)(7)(E) for CONUS use. AWITP instructors must qualify each fiscal year in quarters one or two and quarters three or four at the 85 percent level to maintain proficiency.

g. Training Using Non-Lethal Training Ammunition. Firearms Instructors conducting training using non-lethal training ammunition (FX Marking Cartridge, Ultimate Man Marker Cartridge or equivalent) must attend the basic FITP course and the Firearms Instructor Training for Non–Lethal Training Ammunition Course (ITNTA). NCIS participants shall use only dedicated non–lethal training weapons. These weapons will be permanently converted to fire the training round and the handles and magazine base plates will be painted blue in color. Under no circumstances will the conversion kit be temporarily placed in a duty weapon and the handles taped or designated blue for the duration of that training evolution. In addition, instructors and participants alike must ensure that the training area maintains positive internal controls and that each participant is searched for weapons and live ammo before entry is allowed to the training area. It is imperative that no live ammo or weapons are introduced into the training area.

h. Firearm Safety Rules. Safety rules set forth in this chapter shall apply to all weapons.

(1) Assume every firearm is loaded.

(2) Never point a firearm at anyone or anything you do not intend to destroy or in a direction where an inadvertent discharge may cause harm or injury.

(3) Keep the trigger finger outside the trigger guard until ready to fire.

(4) Always be aware of the target, backstop, and beyond.

(5) When challenged by law enforcement officers who may be responding to reports of an armed subject but are unaware of a special agent's identity, avoid any movements which might be interpreted as threatening or uncooperative. Let the challenging officers or investigators dictate how you are to identify yourself.

CHAPTER 35
TITLE: INCENTIVE AWARDS
POC: CODE 10A
DATE: MAY 08

35-1. INTRODUCTION

The Incentive Awards Program is established to motivate employees to increase productivity and creativity by rewarding those whose job performance is substantially above normal job requirements and performance standards.

35-2. PURPOSE

This chapter provides guidance on the Naval Criminal Investigative Service (NCIS) Incentive Awards Program.

35-3. DEFINITIONS

The definitions applicable to this policy can be found in Department of the Navy (DON) Implementation Guide Number 451-02, Guidance on Implementing Awards Programs. For the purpose of this chapter, an Activity is defined as a NCIS Headquarter's (NCISHQ) departmental code or field office.

35-4. POLICY

The Incentive Awards Program at NCIS adheres to the policy and guidance contained in the DON Civilian Human Resources Manual Subchapter 451.1 and Implementation Guide 451-02, with the following stipulations:

a. NCISHQ Human Resources Directorate, Personnel Operations and Services Department (Code 10A) is responsible for the following:

(1) Serve as the principal point of contact for all administrative matters concerning the Incentive Awards Program; and,

(2) Maintain records and preparing required reports; and,

(3) Ensure that information on the Incentive Awards Program is provided to all new employees during their initial orientation, and that supervisory and managerial training includes the effective use of awards to improve employee performance; and,

(4) Publicize the Incentive Awards Program; and,

(5) Provide technical review and processing award recommendations from all NCISHQ departments and field components.

b. NCISHQ Financial Management Directorate (Code 14) is responsible to budget sufficient funds to cover all categories of cash awards for both agent and non-agent personnel. Amounts budgeted should be based on reasonably objective historical criteria, e.g., dollar amounts and numbers.

35-5. PERFORMANCE AWARD

a. The performance appraisal cycle for all civilian personnel is 01 June - 31 May. Code 10A will notify all components if and to what extent awards will be funded in conjunction with the annual evaluation cycle. Specific guidelines regarding the Performance Award process will also be provided. Performance Award recommendations submitted in conjunction with the annual appraisals must be submitted to Code 10A no later than 01 July.

b. Performance Award documentation. A copy of the performance evaluation must be submitted with a completed Performance Award recommendation, utilizing the template found on the Code 10A website, Appendix (1).

c. Code 10A will notify the originating office of Performance Award decisions.

35-6. SPECIAL-ACT AWARD

a. A Special-Act Award recommendation must be submitted to Code 10A within 30 calendar days following the completion of the act or service prompting the award recommendation.

b. The Special Act Award recommendations must be submitted in memorandum format via the chain of command to Code 10A. Recommendations must specify the amount of the award and provide sufficient information to evaluate the special act being recognized. No performance rating is required.

c. Recommendations for awards should be kept confidential until after approval.

d. An Awards Review Board will be convened to recommend approval or disapproval and the amount of the award.

35-7. HONORARY AWARD

The DON authorizes three Honorary Awards of Merit for its employees. The Navy Distinguished Civilian Service Award (DCSA), the Navy Superior Civilian Service Award (SCSA), and the Navy Meritorious Civilian Service Award (MCSA). Supervisors must submit a complete nomination package no less than 30 days prior to the intended presentation date. The submission package should include the following: a memorandum from the person submitting the nomination, a detailed justification, and the citation (synopsis of the justification). Information on these awards, their purpose and the levels of approval required, may be found on the DON Human Resources website at Awards.

35-8. AGENCY-SPECIFIC AWARDS

The Director, NCIS, has authorized honorary awards which may be presented to NCIS employees and other federal, state, local and foreign law enforcement personnel who are working with NCIS in an investigative capacity within the scope of their assigned duties relating to the NCIS mission. Supervisors must submit nomination packages no less than 30 days prior to intended presentation date.

a. The Medal of Valor is the NCIS supreme award and may be awarded to an individual who distinguished himself or herself with conspicuous bravery or heroism above and beyond the normal demands of the job. To be awarded the Medal of Valor, the nominee shall have performed an act displaying extreme courage while consciously facing imminent peril. Nominations can come from any person witnessing the act. Recommendations will go to the first line supervisor who, in letter format, will forward the recommendation via the management chain. Special Agent in Charge (SAC)/Deputy Assistant Director (DAD) personnel will endorse/non-endorse nominations and shall forward all nominations to the appropriate Executive Assistant Director (EAD). The EAD shall forward the nomination with recommendation to the Deputy Assistant Director for Code 10A. An Awards Review Board, consisting of appointed senior staff, will meet as required and recommendations will be forwarded to the Director for final approval. The medals will be presented by the Director or his designated representative in a ceremonial setting at NCISHQ or within the field office where the recipient was last assigned or detailed, or at a location chosen by the Director.

b. The Medal of Merit is the second highest award and may be awarded to an individual who demonstrated extraordinary service or an exemplary act that resulted in the protection of lives or the direct saving of lives. Nomination procedures are the same as for the Medal of Valor.

c. The Meritorious Unit Commendation (MUC) recognizes outstanding teamwork across NCIS disciplines. The MUC may be awarded to NCIS units that demonstrate meritorious service and resulted in a high value and benefit to the agency beyond that of their peer units. Nominations for the NCIS MUC may be submitted by the first line supervisor via the unit management chain. Nominations shall include a roster of individuals assigned to the NCIS unit. The SAC/DAD shall endorse/non-endorse nominations and shall forward all nominations to the EAD having responsibility for the NCIS unit. The EAD shall forward the nomination with recommendation to the Deputy Assistant Director for Code 10A. An Awards Review Board consisting of senior staff chaired by the Deputy Director (Operations) will meet as required and as directed by the Chairman. The Awards Review Board recommendation will be forwarded to the Director for final approval. The NCIS MUC will be presented by the Director, NCIS, or, a designee, in a ceremonial setting appropriate to the award recipient.

d. The Expeditionary Medal is awarded to personnel upon successful completion of a deployment in support of the OCONUS DON mission in areas in direct support of the Global War on Terrorism (GWOT). This recognition program will be overseen by the NCISHQ Deployment Support Office (DSO). The EAD responsible for the DSO will be the sponsor of the award. Nominations will be administratively supported by code 10A. The DSO will identify those personnel eligible for this recognition and will coordinate with code 10A concerning the execution of applicable nomination and certificate forms. Awardees will receive one medal per deployment. Recognition of NCIS military personnel serving in these areas will be addressed via separate process coordinated by the DSO. No action is necessary by the recipient's supervisor or SAC. Award criteria is as follows:

(1) Awardees must have been deployed to a Combat Contingency Area as designated by the Director, NCIS.

(2) The deployment must have occurred during a time frame identified by the Director, NCIS.

(3) Designated areas and time frames are as follows:

Iraq - 19MAR03 to present
Afghanistan - 01OCT01 to present
Horn of Africa - 01OCT01 to present

(4) A "deployment" in the context of the policy is 90 days of consecutive or accumulative service within the designated country's borders.

Personnel deploying in support of Deployment Availability Roster (DAR) Golf and successive DARs, who otherwise satisfy the award criteria, will be recognized with the NCIS Expeditionary Medal.

e. Nomination for and receipt of one or more of these honorary awards does not preclude an individual from receiving an additional NCIS award, a DON or Department of Defense (DoD) award covering the same period and for the same action which the responsible NCIS supervisor deems appropriate for an award nomination. Futhermore, it does not preclude the deployer from receiving a similar award for the same period of service from a command external to NCIS.

35-9. CIVILIAN OF THE YEAR AWARD

a. The professional and support staff of NCIS continually face new and challenging situations which warrant special recognition. To ensure this occurs, the Director has approved two Civilian of the Year awards to be presented annually to the Administrative Support Civilian of the Year and the Operational Support Civilian of the Year. The Civilian of the Year awards are open to all non-special agent employees at GS-13 and below. Supervisors may nominate employees for this award based on their performance during the preceding performance cycle. Areas of performance to be considered include, but are not limited to:

(1) Professional performance.

(2) Significant accomplishments.

(3) Leadership.

(4) Initiative.

(5) Awards, commendations and other noteworthy achievements.

(6) Productivity.

(7) Organizational support.

(8) Community involvement.

b. The nomination format is provided as Appendix (2). Nomination schedules, special criteria and other specific information will be announced annually via GEN Admin.

c. Nominations will be considered by an Awards Review Panel assigned by the Director and consisting of at least three individuals at or above the GS-14 grade level.

d. After award selections have been made and approved by the Director, the DAD for Personnel Operations and Services will:

(1) Prepare a citation for presentation at a suitable awards ceremony attesting to the selectee’s achievements; and,

(2) Initiate action authorizing payment of a monetary award of $1000.00 for each selectee; and,

(3) Procure and appropriately inscribe a commemorative plaque for each selectee.

e. The Office of Communications will ensure appropriate public recognition of the achievements of the Civilians of the Year.

35-10. SPECIAL AGENT OF THE YEAR AWARD

a. To recognize exceptional professional accomplishments by special agent personnel, the Director has authorized the Special Agent of the Year award. This award is open to all non-supervisory Special Agents in grades GS-13 and below. Awards will be given annually for outstanding performance and investigative expertise in the areas of General Crimes, Fraud, Operations Support, Combating Terrorism and Foreign Counterintelligence.

b. Consideration for selection as Special Agent of the Year will be based on the nominee's achievements during the preceding annual performance cycle. The award year will coincide with the appraisal period ending date (i.e., the 2007 Special Agent of the Year is based on achievements during the 2006 – 2007 performance cycle).

c. Areas of performance to be considered include, but are not limited to:

(1) Professional performance.

(2) Significant accomplishments.

(3) Leadership.

(4) Initiative.

(5) Awards, commendations, and other noteworthy recognition.

(6) Productivity.

(7) Representational ability.

d. The nomination format is provided as Appendix (3). Nomination schedules, special criteria and other specific information will be announced annually via Gen Admin.

e. Nominations will be considered by an Awards Review Panel assigned by the Director and consisting of at least three individuals at or above the GS-14 grade level. The panel will select a minimum of one candidate from each category to be recognized as Special Agent of the Year. If unique and compelling circumstances exist, the panel may select more than one recipient in any or all investigative disciplines. This may be particularly applicable to Special Agents serving in investigative sub-specialties such as polygraph, technical services, forensics, cyber, etc.

f. After award selections have been made an approved by the Director, the Deputy Assistant Director for Personnel Operations and Services will:

(1) Prepare a citation for presentation at a suitable awards ceremony attesting to the selectee's achievements; and,

(2) Initiate action authorizing payment of a monetary award of $1000.00 for each selectee; and,

(3) Procure and appropriately inscribe a commemorative plaque for each selectee.

g. The NCIS Office of Communications, Code 00C, will ensure appropriate public recognition of the achievements of the Special Agents of the Year.

35-11. QUALITY STEP INCREASE

A Quality Step Increase (QSI) provides incentive and recognition for excellence in performance by granting a faster than normal step increase. An employee is eligible for only one QSI within any 52-week period. To receive a QSI, employees must meet the criteria outlined in the DON Implementation Guide 430-02, paragraph 8.b.

35-12. ON-THE-SPOT CASH AWARD

The "On-the-Spot" Cash Award is designed to quickly recognize and provide immediate reinforcement of a one-time achievement by an employee that resulted in service of an exceptionally high quality or quantity. An On-the-Spot Cash Award ranges from $25 to $750, commensurate with the nature of the service or act being recognized. A supervisor initiates the recommendation for On-the-Spot Cash Award for the civilian employee in memorandum format sent via the chain-of-command to Code 10A for review/approval.

35-13. TIME-OFF AWARD

Supervisors at the GS-13 level, or, above, may grant a Time-Off Award without further review for periods not to exceed one workday. Code 10A will review and approve/ disapprove nominations for a Time-Off Award in excess of one workday for NCIS employees worldwide.

35-14. OTHER NON-MONETARY AWARDS

Supervisors may present gift certificates and similar items not to exceed an individual value of $25 to employees whose performance in a particular instance warrants recognition, but not necessarily an On The Spot Cash Award. The specific awards available will vary. Non-monetary awards shall be purchased, tracked and approved by Code 10A2.

35-15. EXCEPTIONAL PERFORMER AWARD

This is a non-monetary recognition program established to provide NCIS employees the opportunity to acknowledge and encourage one another for efforts that promote and reflect employee excellence. All NCIS employees are eligible. Employees may be recognized for such actions as providing exceptional customer service, going the extra mile, i.e., performance above and beyond that required in the normal performance of duties. There is no limit to the number of times an employee can be nominated for an "Exceptional Performer Award" in a given period. The nominator must complete a NCIS Recognition Coupon, provided as Appendix (4) and available on e-forms under the personnel category, list specific examples of what the nominee has done, and select an appropriate lapel pin for the "Exceptional Performer". Code 10A2 will purchase and track the distribution of the pins. No additional approval is required beyond the nominating employee.

APPENDIX (1): PERFORMANCE AWARD RECOMMENDATION FORM TEMPLATE

Employee's Name: _____ **SSN**: _____ **Grade**: _____
Office Code: _____
Period Covered: _____

The above noted employee is hereby recommended for recognition in the form of a Performance Award in the amount of $ _____

Narrative justification for the recommended award is as follows:

First Level Supervisor's Name:
Title:

Signature: _____

Second Level Supervisor's Name:
Title:

Signature: _____

APPENDIX (2): NCIS CIVILIAN OF THE YEAR NOMINATION FORMAT

NAME OF NOMINEE:

OFFICE CODE:

CATEGORY:

BRIEF SUMMARY OF PROFESSIONAL HISTORY:

NARRATIVE (Set forth specific examples of exceptional achievements in the performance areas listed under 35-9.a):

ADDITIONAL PERTINENT INFORMATION, ACTIVITIES, ASSOCIATIONS:

SIGNATURE/TITLE OF FIRST LINE SUPERVISOR:_____

SPECIAL AGENT IN CHARGE/ NCISHQ DEPUTY ASSISTANT DIRECTOR COMMENT:

SIGNATURE/TITLE:_____

APPENDIX (3): NCIS SPECIAL AGENT OF THE YEAR NOMINATION FORMAT

NAME OF NOMINEE:

OFFICE CODE:

CATEGORY:

BRIEF SUMMARY OF PROFESSIONAL HISTORY:

NARRATIVE (Set forth specific examples of exceptional achievements in the performance areas listed under 35-10.c):

ADDITIONAL PERTINENT INFORMATION, ACTIVITIES, ASSOCIATIONS:

SIGNATURE/TITLE OF FIRST LINE SUPERVISOR:_____

SPECIAL AGENT IN CHARGE/ NCISHQ DEPUTY ASSISTANT DIRECTOR COMMENT:

SIGNATURE/TITLE:_____

APPENDIX (4): NCIS RECOGNITION COUPON

Date: _____

To: _____

From: _____

Exceptional Performer Award

Congratulations!!!

Take a bow for going the extra mile.

You deserve a round of applause for excellence and a job well done.

Let me tell you why:

Recognition Coupon

_____

_____ *"Redeemable in _____"*

_____

_____

_____

_____

_____

NCIS-1, Chapter 36
NCIS Security Program
Effective Date: November 2013

Table of Contents

References:

(a) NAVCRIMINVSERVINST 3301.1A, Naval Criminal Investigative Service Emergency Action Plan
(b) SECNAV M-5510.36, Department of the Navy Information Security Program
(c) SECNAV M-5510.30, Department of the Navy Personnel Security Program
(d) DoDM 5200.01, DoD Information Security Program, Volumes 1-4
(e) OPNAVINST 5513.1F, Department of the Navy Security Classification Guides
(f) Executive Order 12968, Access to Classified Information
(g) Executive Order 13556, Controlled Unclassified Information
(h) Intelligence Community Policy Memorandum 2005-700-1
(i) DoDD 8100.02, Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)
(j) Portable Electronic Devices Countermeasures Matrix
(k) Information Assurance Publication 5239-22, Protected Distribution Systems (PDS) Publication
(l) Intelligence Community Directive 705, Sensitive Compartmented Information Facilities
(m) Joint Air Force Army and Navy Manual 6/9, Physical Security Standards for Special Access Program Facilities
(n) NCIS-1, Chapter 26, Facility Management and Engineering
(o) NCIS-1, Chapter 27, NCIS Information Technology
(p) NSA/CSS EPL-02-01-AC, Annex A to NSA/CSS 02-01
(q) NAVSO P-5239-26, Remanence Security Guidebook
(r) DoD 5220.22M, National Industrial Security Program Operating Manual
(s) JAGINST 5800.7F, Manual of the Judge Advocate General
(t) DoDD 5240.06, Counterintelligence Awareness and Reporting (CIAR)
(u) DoDM 5105.21, Sensitive Compartmented Information (SCI) Administrative Security Manual, Volumes 1-3
(v) DoDD 5230.20, Visits and Assignments of Foreign Nationals
(w) Naval Doctrine Publication 1 (NDP-1), Naval Warfare
(x) SECNAVINST 5510.34A, Disclosure of Classified Military Information and Controlled Unclassified Information to Foreign Governments, International Organizations, and Foreign Representatives
(y) Defense Security Service JPAS Account Management Policy
(z) Executive Order 13526, Classified National Security Information
(aa) Navy Department Supplement to DoD DIR S-5105.21-M-1
(bb) Intelligence Community Directive 704
(cc) Director of Naval Intelligence Policy Memorandum, 30 April 2009
(dd) Intelligence Community Directive 705

36-1. Purpose. The purpose of this chapter is to establish policy and provide guidance to NCIS personnel concerning industrial, information, personnel, and physical security, sensitive compartmented information (SCI) and special access programs (SAP).

36-2. Policy. This chapter is applicable to all NCIS military, civilian, and contractor personnel. Portions also apply to personnel from other organizations when visiting NCIS facilities. When fulfilling the requirements of this chapter would result in an untenable sacrifice of operational efficiency, or when there are other good and sufficient reasons for non-compliance, personnel may request a waiver of a specific requirement from the Security Manager via their chain of command. Each request for waiver must give the reason why the requirement cannot be met and describe proposed alternative procedures.

36-3. Cancellation. None.

36.4. Chapter Sponsor. The sponsor for this chapter is the Security Division, Code 11A2.

36-5. Objective. The objective of this chapter is to provide employees with timely and well-written policies that are the framework for protecting classified and sensitive information throughout the agency.

36-6. Definitions. See Appendix (A).

36-7. Responsibilities. The Security Manager, Special Security Officer (SSO), deputy assistant directors (DAD), special agents-in-charge (SAC), assistant directors, executive assistant directors, and Deputy Director are responsible for ensuring compliance with this instruction within their respective areas of responsibility. Each NCIS employee, military, civilian, and contractor, is responsible for compliance with all aspects of this chapter. Specific security program management responsibilities are outlined as follows:

a. Senior Intelligence Officer (SIO). The Director is the SIO and exercises overall responsibility of the SCI program.

b. Original Classification Authority (OCA). See Section 36-9b for OCA information.

c. Security Manager. The Security Manager serves as the advisor to and direct representative of the Director in matters pertaining to all aspects of security within NCIS worldwide.

d. Chief, Security Division. The Chief, Security Division is responsible to the Security Manager for the daily operations of the Security Division.

e. Special Security Officer (SSO). The SSO is responsible to the Chief, Security Division for the daily operations of SCI policy, processes, and programs within the NCIS enterprise. The SSO manages all SCI information, personnel, and physical security functions for NCIS Headquarters and field offices worldwide.

f. Security Programs Manager. The Security Programs Manager is responsible to the Chief, Security Division for the daily operations of collateral security policy, processes, and programs within the NCIS enterprise. The Security Programs Manager manages all collateral information, personnel, and physical security functions for NCIS Headquarters and field offices worldwide.

g. Top Secret Control Officer (TSCO). The TSCO is responsible to the Chief, Security Division for receipt, custody, accountability for, and disposition of all NCIS Top Secret material. The TSCO must be an officer, senior non-commissioned officer E-7 or above, or a civilian employee, GS-7 or above. The TSCO must be a U. S. citizen and have been the subject of an SSBI completed within the previous 5 years.

h. Top Secret Control Assistant (TSCA). Security coordinators in each headquarters code and field office are further designated as a TSCA. The TSCA is responsible to the DAD or SAC and the TSCO for receipt, custody, accountability and disposition of all Top Secret material within their geographic area of responsibility. The DAD or SAC may designate additional TSCAs as necessary due to the geographic location of Top Secret material that may be remote to the field office. Notification of additional TSCAs will be provided to the Security Manager in writing. Persons designated as TSCAs must be U. S. citizens and either an officer, enlisted person E-5 or above, or civilian employee GS-5 or above. An established Top Secret security clearance eligibility is required.

i. NATO Control Officer. The NATO Control Officer is responsible to the Security Manager for receipt, custody, and accountability for the disposition of all NATO material held by NCIS.

j. Information Assurance Manager (IAM). The IAM serves as the point of contact for all command information assurance (IA) matters and implements the command's IA program.

k. Information Assurance Officer (IAO)/System Administrator. An IAO or system administrator will be appointed for each information system and network in the command and will be responsible for implementing and maintaining the command's information assurance requirements.

l. Special Security Representative (SSR). DADs and SACs will designate a properly cleared and indoctrinated SSR, minimum grade GS-9, where the code or field office houses a Sensitive Compartmented Information Facility (SCIF), and delegate sufficient authority for the SSR to properly manage the SCI security program of the respective office. The SSR is responsible to the DAD, SAC and SSO for all matters pertaining to SCI security within their geographic area of responsibility. The DAD or SAC may also designate a security coordinator/assistant security coordinator as the SSR as deemed appropriate.

m. Security Coordinators. Each headquarters code and field office will designate a primary security coordinator, minimum grade GS-7, military officer, or enlisted E-7 or above and one or more assistant security coordinators, minimum grade GS-6 or E-6. Such designation should be made, in writing, to the Security Manager, Code 11A. In addition, appoint an assistant security coordinator at each subordinate unit. Such designation is made, in writing, by the DAD or SAC

and a copy maintained at the parent unit. Security coordinators and assistant security coordinators are responsible to their DAD or SAC and the Security Manager for matters pertaining to the security of classified information related to their respective codes and field offices. They will be delegated sufficient authority to properly manage their respective security requirements.

n. Security Procedures and Emergency Action Plans (EAP). Reference (a) is the EAP for all NCIS offices within the Marine Corps Base Quantico area of responsibilities. Each field office and subordinate unit is required to use reference (a) as a template to develop an EAP for the protection of classified material in case of natural disaster, civil disturbance, or enemy action. The EAP must provide for the protection of classified information in a way that will minimize the risk of loss of life or injury to personnel. Plans should call for immediate evacuation in case of fire and not require that all classified information be properly stored before leaving. Placing a perimeter guard and controlling access to the area will provide sufficient protection and reduce casualty risk. In developing an EAP, the component's vulnerability should be reviewed for situations that could result in the compromise of classified information. Emergency planning and evaluation of vulnerabilities should include consideration of the issues addressed in reference (b), Exhibit 2B.

o. Standard Operating Procedures

(1) Each headquarters code and field office is required to prepare and maintain written security standard operating procedures specifying how the requirements of this chapter will be accomplished, in the component, using reference (b), Exhibit 2A, as a guideline. Each component may not be involved with all phases of the security program, but there are some elements common to all. These include the following but are not limited to:

(a) Accounting and control of classified information.

(b) Physical security measures for protection of classified information.

(c) Control of reproduction, destruction, and screening of incoming material until determination of classification status is made.

(d) Control of visitors.

(2) Each component's security procedures should include special precautions for extraordinary security control measures that need to be observed. Particular attention should be paid to applying basic security policy wherever automated data processing equipment is used for processing classified information.

p. Inspections

(1) The Security Division conducts Staff Assistance Visits (SAVs) to evaluate the overall effectiveness of the agency's security program. Each headquarters code and field office will receive a SAV approximately every 24 months. Security Division personnel will examine

overall security management and procedures for management, accounting and control of classified information, physical protection of classified information, personnel security, and security awareness and education.

(2) Primary security coordinators should conduct SAVs at subordinate units at least six months prior to scheduled Inspector General (IG) inspections and Security Division SAVs. Maintain the results of subordinate unit SAVs at the main code or field office. Security Division inspectors will review the results during scheduled inspections.

(3) The Security Division and security coordinators will conduct unannounced inspections to evaluate compliance and identify weaknesses or deficiencies in the overall security program.

(4) The Security Division may support IG inspections. Regardless of the level of involvement of the Security Division, all security-related findings from IG inspections will be reported to the Security Manager. The Security Division will send a separate, more comprehensive report, based on the SAV Checklist, to the SAC or DAD. Contact the Security Division to obtain a copy of the SAV Checklist. The Security Division report will be in addition to the information contained in the IG report.

(5) The Security Manager will report SAV, IG and unannounced inspection results to the SAC or DAD.

36-8. Security Education

a. Basic Policy. The Security Division will provide all NCIS personnel, regardless of position, rank, or grade with education in security policies and procedures on a continuing basis.

b. Responsibilities. The Security Manager is responsible for formulating and coordinating security education. In addition to rendering assistance and instruction on a case-by-case basis, the Special Security Officer and Security Programs Manager ensure the briefings described in section 36-8c are scheduled and presented when required.

c. Training. The following training is included in the Security Education and Awareness Program:

(1) Indoctrination. These briefings are conducted per reference (c), paragraph 4-5, when NCIS is the first active duty assignment for military personnel or the first government appointment for civilian personnel. Contractors assigned to NCIS codes or field offices receive indoctrination training from their company.

(2) Security Orientation Training. All personnel are provided an initial security orientation brief upon reporting to NCIS. This orientation will include reporting responsibilities and NCIS specific requirements for protecting classified information.

(3) Annual Security Refresher Training. All personnel who have access to classified information shall receive annual security refresher training. Refresher training is based on information contained in reference (c), paragraph 4-8. Refresher training is given once a year and as required. Refresher training will be in the form of computer-based training, e-mail or in person, as determined by the Security Division. Participation by all military, civilian and contractor personnel is mandatory.

(4) Classification Management

(a) Original Classification Authority (OCA). The Chief, Security Division will provide training to the OCA upon initial appointment and annually thereafter. The training will be given per reference (b), Chapter 4.

(b) Security Classification Guides (SCG). The Security Division will provide initial and refresher training to subject matter experts (SME) who support the OCA in creating and updating SCGs. Training will include SCG format, marking guidelines and declassification instructions. Additionally, SMEs will complete on-line training, identified by the Security Division, through the Defense Security Service (DSS).

(c) Derivative Classifiers. All other personnel must receive training in derivative classification prior to gaining initial access to classified information. In addition, they must receive refresher training in derivative classification every two years.

(d) Declassification Authority. Personnel appointed as Declassification Authorities must complete on-line training, identified by the Security Division, through DSS. In addition, the Security Division provides an initial briefing. Refresher training is conducted every two years.

(e) Special Briefings/Training. The Security Division provides other special briefings such as for foreign travel, courier duties, and special access programs (SAP), as needed. Briefings tailored to specific codes and field offices are also conducted. These briefings do not replace the requirement for the annual refresher briefing.

(f) Security Coordinators .

1. Security coordinators receive initial training from the Security Division upon assignment. Follow-up training is conducted during quarterly security coordinator meetings and during visits.

2. Each security coordinator briefs newly assigned personnel concerning their individual security responsibilities tailored to the particular area to which assigned. Topics found in Appendix (A), Newcomer Indoctrination/Orientation Guide and Appendix (B), On-The-Job Briefing Guide should be covered.

d. Supervisors. On-the-job training will include instruction relative to security procedures appropriate for the assigned position. Supervisors will ensure, as a minimum, that the topics found in Appendix (A), Newcomer Indoctrination/Orientation Guide and Appendix (B) On-The-

Job Briefing Guide are fully covered and understood. Supervisors are accountable for procedural violations and/or for compromises that result from improper training of personnel. Reference (c), paragraph 4-7 applies.

e. Operations Security (OPSEC). OPSEC is separate and distinct from physical, information, personnel and other traditional security disciplines. It focuses on the protection of information and operations from unauthorized disclosure to adversaries and prevents or reduces inadvertent release of sensitive but unclassified information to persons not having a need-to-know. OPSEC is an integral part of NCIS operational activities. Training, as it pertains to the conduct, support and administration of operational activity, is addressed in those relevant operational policies and guidelines. The Security Division will incorporate OPSEC information into the Annual Security Refresher Training. Notwithstanding operational activity-related OPSEC, it is incumbent upon all NCIS personnel to apply the basic premises of security awareness to all phases of NCIS business, regardless of classification, in order to avoid potential compromise of NCIS methods of operation, privacy protected data or other law enforcement sensitive information.

f. Debriefings. Personnel with access to classified material will be debriefed prior to termination of active military service or civilian employment, or upon revocation or withdrawal of security clearance.

36-9. Classification Management

a. Classification Levels. Information requiring protection against unauthorized disclosure in the interest of national security is classified at the Top Secret, Secret, or Confidential levels. Except as otherwise provided by statute, do not use terms such as “For Official Use Only” (FOUO), “Law Enforcement Sensitive” (LES) or “Secret Sensitive” (SS) to identify United States classified information.

(1) Top Secret. Top Secret is the classification level applied to information whose unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to national security. Examples include information whose unauthorized release could result in armed hostilities against the United States or its allies; a disruption of foreign relations vitally affecting the national security; the compromise of vital national defense plans; the disclosure of complex cryptographic and communications intelligence systems; the disclosure of sensitive intelligence operations; and the disclosure of significant scientific or technological developments vital to national security.

(2) Secret. Secret is the classification level applied to information whose unauthorized disclosure could reasonably be expected to cause serious damage to the national security. Examples include information whose unauthorized release could result in the disruption of foreign relations significantly affecting the national security; the significant impairment of a program or policy directly related to the national security; the disclosure of significant military plans or intelligence operations; and the disclosure of scientific or technological developments relating to national security.

(3) Confidential. Confidential is the classification level applied to information whose unauthorized disclosure could reasonably be expected to cause damage to the national security. Examples include information whose unauthorized release could result in disclosure of ground, air, and naval forces (e.g., force levels and force dispositions); or disclosure of performance characteristics, such as design, test, and production data of United States munitions and weapons systems.

(4) Controlled Unclassified Information. Unclassified information that requires safeguarding or dissemination controls is known as controlled unclassified information (CUI). Reference (d), Volume 4 and reference (b), Chapter 8, identify several types of information as CUI. The ones most commonly used in NCIS are:

(a) For Official Use Only (FOUO). FOUO is a designation used by DoD and a number of other Federal agencies to identify information or material, which although unclassified, may not be appropriate for public release. FOUO information may be disseminated within DoD components and between officials of the DoD components and DoD contractors, consultants, and grantees as necessary in the conduct of official business. FOUO information may also be released to officials in other departments and agencies of the executive and judicial branches in performance of a valid government function.

(b) Law Enforcement Sensitive. LES is a marking sometimes applied, in addition to or in conjunction with the marking FOR OFFICIAL USE ONLY, by the Department of Justice and other activities in the law enforcement community. This marking denotes that the information was compiled for law enforcement purposes and should be afforded appropriate security in order to protect certain legitimate government interests, including the protection of:

1. Law enforcement proceedings.

2. The right of a person to a fair trial.

3. An impartial adjudication.

4. Grand jury information.

5. Personal privacy including records about individuals requiring protection under the Privacy Act.

6. The identity of a confidential source, including a State, local, or foreign agency.

7. Authority or any private institution which furnished information on a confidential basis.

8. Information furnished by a confidential source.

9. Proprietary information.

10. Techniques and procedures for law enforcement investigations or prosecutions.

11. Guidelines for law enforcement investigations or prosecutions.

12. Guidelines for law enforcement investigations when disclosure of such guidelines could reasonably be expected to risk circumvention of the law.

13. The life or physical safety of any individual, including law enforcement personnel.

(c) Foreign Government Information (FGI) is information provided to the U.S. Government by a foreign government or governments, an international organization of governments, or any element thereof, with the expectation that the information, the source of the information, or both, are to be held in confidence.

1. Classified FGI retains its original classification level or is assigned a U.S. Government classification equivalent per reference (b), Exhibit 6C. The responsibility to assign the U. S. classification belongs to the receiver. Mark classified FGI per reference (b), paragraph 6-16.

2. Mark Restricted FGI per reference (d), volume 4. It may be classified at a higher level if it meets the damage criteria of reference (b), paragraph 4-2.

b. Original Classification Authority. Original classification is the initial determination that information requires protection against unauthorized disclosure. Original Classification Authorities (OCA) makes these decisions. OCAs are designated by virtue of their position. The Director is the only OCA within NCIS. This OCA authority is not transferable and shall not be further delegated.

c. Derivative Classification

(1) Derivative classification is the incorporating, paraphrasing, restating, or generating, in new form, information that is already classified. Using an SCG to classify information is a derivative classification decision.

(2) The new form of information must be marked consistent with the classification markings that apply to the classified source. For example, when a classified report is compiled, using several classified source documents as a basis, the classification markings associated with the source documents must be carried forward to the new report. The writer of the new report is the derivative classifier, not the OCA. Nearly all classified documents created within NCIS are derivatively classified.

(3) It is the individual responsibility of the derivative classifier to observe and respect the original classification determination of the source and to carry forward to any newly created information the pertinent classification markings.

(4) Derivative classifiers are accountable for the accuracy of their classification decisions. NCIS personnel with signature authority are responsible to ensure that classification markings are correct prior to signing documents prepared by derivative classifiers.

(5) Refer questionable derivative classification decisions to the Security Division for resolution by the Security Manager.

d. Classification Challenges

(1) Forward any information believed to be improperly classified to the Security Division for resolution.

(2) The Security Division will contact the Command Security Manager where the information originated to resolve the issue.

(3) Refer classification challenges to information originated by NCIS to the Security Division for resolution.

e. Declassification Review

(1) Declassification Authorities (DA) are appointed by the Director as declassification reviewers of classified information with NCIS equity. Each DA is responsible for performing classification reviews of requested documents to ensure national security information (NSI) is protected at the appropriate classification level. Most of the material will be based on counterintelligence, counterterrorism and/or cyber investigations.

(2) DAs receive requests for declassification review from headquarters departments and, in some cases, from field offices.

(a) The DA will review the documents using the appropriate SCG. Once the review is complete, the DA will:

1. Declassify, downgrade, upgrade or forward the documents unchanged.

2. Remark the documents, as appropriate, and annotate the authority line, if necessary.

3. Forward documents that do not have clear declassification guidance to the OCA for a decision. Work with subject matter experts, familiar with the subject, to provide the OCA with a suggested decision.

4. Complete a memorandum detailing the classification determination made for the documents.

5. The Security Division will review the documents for proper classification markings and to ensure the correct declassification decision was made.

36-10. Security Classification Guides (SCG)

a. SCGs record original classification determinations promulgated from the OCA. SCGs are the primary reference source for derivative classifiers to identify the level and duration of classification for specific information elements.

b. The vast majority of information derivatively classified within NCIS can be correctly accomplished using four primary SCGs located on the Multiple Threat Alert Center webpage on SIPRNET:

(1) OPNAVINST 5513.4E, SCG ID# 04-5.1, DON Security and Investigative Matters

(2) *OPNAVINST 5513.4E, SCG ID# 04-17.2, DoD Counterintelligence (CI) Program

(3) OPNAVINST 5513.4E, SCG ID# 04-25.1, Emerald Quest/Sentinel System

(4) OPNAVINST 5513.4E, SCG ID# 04-29.1, Human Derived Information

***NOTE**: DoD S-5240.09-M, Offensive Counterintelligence Operations Procedures and Security Classification Guide (U), may also be used as a source document for counterintelligence operations when there is no clear guidance contained in OPNAVINST 5513.4E, SCG ID# 04-17.2.

c. The format for each SCG will follow the formatting and marking criteria set forth in references (d) and (e) respectively.

d. Original Classification Authorities must review SCGs every five years for accuracy. The Security Division will forward each SCG via the internal tasking system to the appropriate code or codes for review/update. Each code will ensure all information in the SCG, under their respective area of responsibility, is still relevant to the actions performed by NCIS. The code will also ensure the proper classification of each SCG and that the information contained within is properly marked.

e. Prior to sending any classification guide forward for approval, the Security Division will:

(1) Ensure each SME completes OCA training as identified by the Security Division.

(2) Meet with SMEs prior to the SCG being sent forward to ensure the SCG meets all requirements set forth in the references (d) and (e).

(3) Coordinate the review process for each SCG.

36-11. Marking

a. All NCIS personnel are personally and individually responsible for properly protecting classified information and CUI under their custody and control. Classified information will be marked per reference (d), volumes 2 and 4, and reference (b), Chapter 6.

b. All NCIS personnel are derivative classifiers. Derivative classifiers use source documents to make classification determinations and apply associated markings. Source documents come in the following forms:

(1) Previously classified documents.

(2) Security classification guides.

c. Documents created by NCIS derivative classifiers must contain all of the elements prescribed in references (b), (d), (f) and (g). The elements include:

(1) Banner lines provide overall classification and associated markings and are located at the top and bottom of each page.

(2) Portion markings annotate the classification level of the subject, title, paragraphs, tables and other portions of a document.

(3) The classification authority block is normally located on the face of derivative documents. In cases where software programs do not allow this information to be located on the face, place it at the end of the document in a position that makes it easy to locate. The classification authority block consists of the following:

(a) “Classified By:” line.

(b) “Derived From:” line.

(c) “Declassify On:” line.

(d) Personnel may also carry over other declassification and downgrading instructions from source documents, SCGs or other guidance from an OCA.

d. Multiple Sources

(1) When derivative classifiers use more than one source for determining the classification of the documents, they must list the sources for future reference.

(2) List all sources on the face of the document, if there is enough space. When space is limited, list the sources in the reference section of the document (if there is one) or on a separate sheet.

(3) When a separate sheet is used, keep the multiple source list with the record copy of the document. Derivative classifiers must make this list available to other personnel upon request.

e. Promptly return improperly marked classified information received from outside organizations to the sender for proper marking. In lieu of return, the receiver may contact the sender for proper marking guidance and mark the information accordingly. Maintain a record of this event with the file copy of the remarked information.

f. Do not incorporate improperly marked classified information, regardless of the source, into NCIS-generated classified information or allow it to become part of a permanent record.

36-12. Safeguarding

a. Responsibility for Safeguarding

(1) Anyone who has possession of classified materials is responsible for safeguarding it at all times, and for securing it in appropriate security containers whenever it is not in use or under direct supervision of authorized personnel. Do not leave classified material unattended in offices or areas within NCIS, unless specifically authorized.

(2) Appropriately cleared personnel must protect classified material that has been removed from storage to safeguard it from loss or compromise. Locked offices, whether secured by key lock or cipher lock, do not afford the level of protection required to safeguard classified material during duty or non-duty hours. Properly store all classified material in an authorized security container, or in a facility approved for open storage, when it will no longer be under the direct supervision of authorized personnel.

(3) Personnel working in NCIS facilities at the Russell-Knox Building (RKB) will maintain a clean desk policy. Desktops will be free of classified and sensitive information and it will be stored in a GSA-approved security container, locked desk or filing cabinet. Classified and unclassified information will not be collocated in the same drawer. DADs and SACs are encouraged to implement the same policy at headquarters entities not located in the RKB and field offices (including subordinate units). Specific information relating to the protection of classified material is further defined in facility accreditation, approval and certification documents.

(4) Personnel will not remove classified material from NCIS facilities except in the performance of official duties and under conditions providing the protection required by reference (b), Chapter 9. The Security Division (for headquarters personnel) and SAC (for field office personnel) will authorize classified information to be transported through the approval of a courier card. Approval to transport classified information on a commercial airline is promulgated through a courier authorization letter.

b. Escorting. Employees must pay particular attention to non-cleared personnel performing tasks within facilities where classified and sensitive information is processed.

(1) Escorts will be assigned at a ratio not to exceed one escort for every five workers.

(2) All escorts shall:

(a) Keep visitors in their line of site to ensure that workers remain clear of classified areas.

(b) Be dedicated and focused solely on the task and not engage in any other activities (e.g. assisting cleaning and maintenance personnel in the performance of their assigned tasks).

c. Procedures for the Security of Classified Laptops

(1) Secret Agent Software (SAS) and Mobile Armor are software programs used to protect national security information. One of the two programs is installed on all NCIS laptops approved for processing classified information up to Secret. They must be used in addition to the requirements contained in reference (b), Chapter 9.

(2) When removing classified laptops from NCIS facilities, store them in an authorized storage container per reference (b), Chapter 10 when not in use.

(3) Make a reasonable effort to store laptops in approved security containers; however, when deployed to forward areas where the security requirements of reference (b), Chapter 10 cannot always be provided, follow the compensatory measures outlined below:

(a) Dedicate specific laptops for deployment.

(b) Disable network adapters and Universal Serial Bus (USB) controllers.

(c) Erase hard drives prior to deployment and load only with the required classified material.

(d) Deploying personnel will receipt for the laptop and hard drive and conduct an inventory of classified material on the hard drive.

(e) During the deployment and when the classified hard drive cannot be secured per reference (b), Chapter 10, the deployed personnel will keep the laptop on his/her person or in sight/control at all times.

(f) Security coordinators will brief deploying personnel on their responsibilities to protect classified information.

(4) Upon return, deployed personnel will complete the following tasks:

(a) Properly secure the laptop and hard drive.

(b) Inventory classified material located on the hard drive and compare to the original inventory to assure completeness.

(c) Transfer unclassified and classified material from the hard drive to the appropriate computer storage systems/media.

(d) Erase the hard drive and make the laptop available for the next deployment.

d. Identification Cards and Badges

(1) The Visitor Control Center for the RKB will issue identification badges to all individuals requiring access to the building.

(a) NCIS government personnel needing an RKB badge will contact the Security Division directly.

(b) NCIS contractor requests for badges must come from the contracting officer's representative (COR). The COR must ensure the contractor's facility security officer sends a visit request in JPAS (via letter, e-mail, or fax when JPAS is unavailable). Additionally, a DD 254 must be on file in the Security Division.

(c) Non-NCIS visitors must have their security office send clearance verification via JPAS using one of the following Security Management Office (SMO) codes (they may send a letter, e-mail, or FAX when JPAS is unavailable):

1. SMO Code "RKB" for collateral visits.

2. SMO Code "RKBSCI" for SCI visits.

(2) Check with your security coordinator for badge procedures at field offices and other subordinate locations.

(3) Personnel must display badges above the waist while inside NCIS facilities.

(4) Immediately report lost or stolen ID cards or badges to your security coordinator or the Security Division.

e. Care of Working Spaces

(1) Do not place or store extraneous material (papers, printouts, publications, etc.) on top of security containers.

(2) When printing or copying documents containing classified or sensitive information, be sure to immediately remove the documents from the printer or copier, to preclude access by non-cleared personnel or cleared personnel who do not have a need-to-know.

f. Care During Working Hours

(1) Keep classified documents under constant surveillance when they are removed from storage for working purposes and affix with the appropriate cover sheet. Approved cover sheets include Standard Forms (SF) 703, 704, and 705 for Top Secret, Secret, and Confidential documents, respectively.

(2) Do not discuss classified information when unauthorized persons can overhear the discussion. Take particular care in partitioned office spaces and when there are visitors, cleaning or repair personnel present.

g. Security Checks

(1) Conduct security checks at the end of each working day and when completing work after normal duty hours, on weekends or on holidays, to make sure all spaces, classified and sensitive material, and computers are properly secured.

(2) Post SF 701, Activity Security Checklist, just inside the main entrance, to record security checks. List security containers by number. Other items that should be added to the standard checklist are STE cards, burn bags, and other items deemed appropriate.

(3) Use SF 702, Security Container Check Sheets, to record each time a security container or open storage area is opened, closed, or checked. When conducting security checks make sure that:

(a) All classified material is stored in the manner prescribed in reference (b), Chapter 7.

(b) Burn bags are properly stored.

(c) Classified notes, rough drafts, typewriter ribbons and AIS media are properly secured.

(d) Security containers have been locked and checked. Rotate the dial of combination locks at least four complete times, in the same direction, when securing security containers, open storage areas, and SCIFs. Each drawer of a security container should be physically checked once the combination lock dial has been rotated to ensure each is properly secured.

h. Security Containers

(1) Display a reversible "OPEN/CLOSED" or similar sign on all security containers and secure spaces.

(2) Place the sign on the locking drawer or adjacent to the combination lock of the entrance door, as appropriate.

(3) The sign will indicate the correct status of the security container or secure space.

i. Top Secret (TS) Control Procedures

(1) Continuously account for all collateral TS material originated or received. Notify your security coordinator, who also serves as the TSCA, of all TS material processed in hardcopy form. This does not include Top Secret documents that are printed and destroyed on the same day.

(2) The TSCA will individually serialize, log it into the local Top Secret Control Log and notify the TSCO at the Security Division. The TSCO will then enter the information into the command Top Secret Control Log.

(3) Top Secret information will be accounted for by a continuous chain of receipts. Hand-to-hand transfer for internal distribution within headquarters will be effected by notifying the TSCO to update the command's accountability register.

(4) When no longer needed, destroy TS information per reference (b), Chapter 10. Two appropriately cleared individuals are needed to perform this duty. Inform the TSCA (security coordinator) of the destruction so they can annotate the local TS control log and notify the TSCO. Retain all destruction records for a period not to exceed five years from the date of destruction.

(5) Personnel must obtain permission to reproduce TS information from the originating agency or higher authorities where applicable.

(6) Security coordinators will conduct annual TS inventories during the month of December using the TS Control Log.

(a) Forward the logs to the TSCO when updates are made and in conjunction with the annual TS inventory.

(b) Report the results of the TS inventories to the TSCO in January of the following year. The TSCO will compile the inventory information and furnish the results, in a formal report to the Director, via the Security Manager.

j. Secret and Confidential. Secret and Confidential information require protection from unauthorized disclosure by access control and compliance with the marking, storage, transmission, and destruction requirements of reference (b), Chapter 10.

k. Removable Automated Information Systems (AIS) and Storage Media

(1) Removable information storage media and devices used with AIS, typewriters, computers, and laptop computers, must be accounted for and controlled based on the highest level of classified information contained therein.

(2) Such media will be marked externally per reference (b), Chapter 6, by using colored labels (Standard Forms 706, 707, 708, 709, 710 and 711) that clearly indicate the classification level and associated markings of the information they contain. Unclassified media will be marked as unclassified. Commercially purchased unclassified software, which is appropriately labeled as commercial software, need not be additionally marked as unclassified.

l. Controls on Reproduction

(1) Do not reproduce Top Secret information without the consent of the originator. Individually inventory all copies of TS documents kept overnight, in the same manner described in paragraph 36-12i above.

(2) Authority to reproduce Secret and Confidential information is delegated to the custodian of the material. Custodians will observe all reproduction prohibitions and ensure that the reproduction of classified material is kept to an absolute minimum. Custodians will coordinate reproduction of classified NATO documents and/or documents marked with special dissemination and reproduction limitations with their TSCA. Do not reproduce NATO documents without the consent of the NATO Control Officer located in the Security Division.

36-13. Portable Electronic Devices (PED)

a. References (h) and (i) establish the National Intelligence Community and DoD policy on the use of PEDs. These documents mandate that agencies take steps to control the introduction and use of PEDs, associated electronic media, and auxiliary equipment in a restricted access area (RAA), controlled access area (CAA), secure room (secret open storage), sensitive compartmented information facility (SCIF) or special access program facility (SAP-F) where classified information is electronically processed or discussed. Use reference (j) as a guide for the introduction and use of PEDs in these facilities.

b. Implementation of this policy requires the coordinated efforts of all employees as indicated below:

(1) The Command Information Officer (CIO), on behalf of the Director, shall:

(a) Provide management and oversight of the NCIS information assurance (IA) program, including development and implementation of IA policies and procedures.

(b) Review and approve planned acquisitions of government procured PEDs.

(c) Provide IA technical guidance for securing government procured PEDs.

(d) Provide IA technical guidance for the proper introduction and use of government-procured PEDs in NCIS facilities.

(e) Provide IA technical guidance for the use of contractor-issued PEDs.

(f) Review and recommend updates to reference (b), as vulnerabilities are discovered.

(g) Develop and provide initial and annual NCIS IA awareness training for the NCIS workforce to address current PED vulnerabilities and threats.

(h) Perform electronic monitoring and report PED use and violations within NCIS facilities.

(2) The Security Manager shall:

(a) Ensure personnel do not bring unauthorized PEDs into the secured areas of NCIS facilities and perform random inspections to ensure compliance.

(b) Initiate a preliminary inquiry, to include confiscation of the PED or PEDs in question, for the following violations:

1. Introducing an unauthorized PED into a RAA, CAA, secure room (secret open storage), SCIF or SAP-F where classified information is electronically processed or discussed.

2. Failure to provide supporting documentation to security personnel upon request (such as an authorization letter).

3. Using a PED to conduct voice or data communication while in a secured area within a NCIS facility, except per reference (j).

(d) Seize evidence pertaining to the unauthorized presence or use of PEDs and removable media.

(e) Approve waivers for alternate placement of storage containers where space limitations prevent storage of PEDs before primary entry and exit points.

(f) In coordination with the CIO, develop policies and provide guidance regarding the introduction and use of PEDs within NCIS facilities.

(3) The COR shall:

(a) Provide initial approval when contractor-issued PEDs serve a justified mission requirement in support of NCIS contracts, and ensure devices and usage are documented within the statement of work and annotated on the DD Form 254.

(b) Request authorization from the Security Manager to bring contractor-issued PEDs into and out of NCIS facilities where classified information is processed.

(4) Headquarters code and field office security coordinators shall:

(a) Oversee implementation of this policy within their respective codes or field offices.

(b) Coordinate with the Security Manager and CIO to resolve questions or concerns relating to this policy.

(c) Report violations of this policy to the Security Division.

(5) The NCIS workforce shall:

(a) Adhere to the procedures and requirements in this policy.

(b) Not connect any PED to NCIS telecommunications networks, information systems, telephony, or Ethernet without prior written authorization from the Security Manager.

(c) Use only authorized PEDs in areas of NCIS where classified information is processed.

(d) Protect government-issued and contractor-procured PEDs from unauthorized access or theft.

(e) Report any violation or suspected violation of this policy to the Security Manager.

c. All personnel must follow the procedures below to be in compliance with the PED policy:

(1) All NCIS personnel and visitors with government-owned PEDs shall comply with the PED security safeguards described in reference (j).

(2) All NCIS personnel and visitors with personally-owned PEDs shall leave unauthorized PEDs outside of NCIS spaces where classified information is electronically processed or discussed. When this is impractical, such as when individuals use public transportation, PEDs must be stored in a NCIS-provided storage locker. Lockers will be located adjacent to primary entry points and other non-discussion areas.

(3) Personally-owned thumb drives, compact discs (CDs), and digital video discs (DVDs) - such as homemade CDs and DVDs - are prohibited from NCIS facilities. However, commercially-manufactured, mass-produced CDs and DVDs which contain the manufacturer's label are permitted within NCIS facilities, but shall not be inserted into NCIS information systems.

(4) The unauthorized use of removable media and PEDs threatens the survivability of NCIS information systems and the performance of NCIS's mission. Violations of the appropriate use of removable media or PEDs will be aggressively pursued. The unauthorized possession or use of a PED may result in its confiscation by NCIS officials for the purpose of conducting a forensic or physical examination.

(5) A forensics inspection will result in examination of all content metadata residing on the PED.

(6) There is no reasonable expectation of privacy or confidentially in the content and metadata resident on PEDs brought into NCIS facilities.

(7) Authorized examination of PEDs may result in data loss, compromise of PED functions, and damage or destruction of the PED. PEDs seized as evidence of a crime or security violation will be handled under DoD and NCIS policies. In some cases, PEDs may be permanently retained, destroyed, or have their data operating systems sanitized.

(8) The PED, in some cases, may not be returned to the user at the discretion of the SIO.

(9) Government-issued PEDs are subject to the security safeguards described in reference (j).

(10) Government-issued PEDs which contain sensitive information (classified or unclassified) must be encrypted with a National Security Agency or DoD-approved encryption standard.

(11) Mission-critical contractor PEDs used in support of NCIS contracts are subject to the same restrictions as government-issued PEDs. Contractor-provided PEDs and intended usage must be included in the Statement of Work and documented in a valid DD Form 254.

(12) The prohibition against introducing electronic equipment into NCIS facilities does not apply to:

(a) Items needed by the disabled or for medical or health reasons, such as motorized wheelchairs, hearing aids, heart monitors, pacemakers, and insulin pumps, etc. However, other health or medical equipment which require connection to an IS must first be approved by the Security Manager prior to their introduction into any NCIS facility. Personnel having questions regarding what type of medical equipment can be introduced into NCIS facilities without an advanced approval shall seek guidance from their security coordinator.

(b) Emergency and police personnel and their equipment, including devices carried by emergency medical personnel responding to a medical crisis within a NCIS facility. Emergency personnel will be admitted without regard to their security clearance status but must be escorted to the degree practical. If appropriate, emergency personnel will be debriefed as soon as possible if there are any indications these individuals have been exposed to classified information or information systems.

(c) Compromising emanations TEMPEST testing equipment or technical surveillance countermeasures testing equipment, as long as the personnel operating the equipment are certified and possess the appropriate security clearances and SCI indoctrination.

36-14. Dissemination of Classified Material

a. Top Secret Material. Do not disseminate, transfer, loan or share, Top Secret material without the prior approval of the originator of the information.

b. Secret and Confidential Material. Secret and Confidential material may be disseminated, transferred, loaned, or shared, without any prior approval, to other DoD and executive branch components, to those with a commensurate clearance and need to know, unless otherwise restricted. See reference (d), Volume 3, Enclosure (2), for guidance on restrictions outside of the executive branch.

c. NATO Material. Do disseminate, transfer, loan or share NATO material without the prior approval of the NATO Control Officer.

d. For Official Use Only (FOUO). FOUO information may be disseminated within the DoD components and between officials of the DoD components and DoD contractors, consultants, and grantees as necessary in the conduct of official business. FOUO information may also be released to officials in other departments and agencies of the executive and judicial branches in performance of a valid government function.

e. Prepublication Review

(1) Clearance of information proposed for publication. Information proposed for publication or public release that concerns or affects the plans, policies, programs, or operations of the DoD, the DON or the U. S. Government, and that is prepared by NCIS personnel either in an official or private capacity, shall be submitted to the Security Division for coordination for review and clearance prior to publication. Coordination with the Communications Directorate, Code 00C, via Deputy Under Secretary of the Navy (DUSN) (Plans, Policy, Oversight and Integration (PPOI)), Security Directorate (SD), is necessary if the information falls into any of the categories in reference (b), Exhibit 8B.

(2) Submit the information for review when in doubt as to whether the information proposed for publication requires clearance.

(3) The speaker or author must initial a speech, article or paper being submitted for review to indicate approval of the text.

(4) Forward articles, books, speeches, etc. to the NCIS Security Division for review not less than 30 working days before the date clearance is desired.

(5) Submit the full and final text of material requiring review, including any supplemental audiovisual material.

(6) Notes, abstracts or outlines will not be accepted to process for clearance as a substitute for a complete text.

(7) Security and Policy Review. The NCIS Security Division will coordinate material submitted for clearance for public release with DUSN PPOI/SD and/or other cognizant authorities as required by reference (b), Chapter 8.

36-15. Transmission and Transportation of Classified Material

a. Top Secret. Transmit or transport Top Secret material by:

(1) Utilizing STE terminals and transmission systems authorized for, as a minimum, Top Secret transmission.

(2) The Defense Courier Service.

(3) Cleared and designated military, civilian or contractor personnel traveling on a conveyance owned, controlled or chartered by the Government or a DoD contractor.

(4) Cleared and designated military, civilian or contractor personnel traveling by surface transportation.

(5) Cleared and designated military, civilian or contractor personnel on scheduled commercial passenger aircraft within and between the United States, its Territories and Canada, when approved by the Security Division.

(6) Cleared and designated military, civilian or contractor personnel on scheduled commercial passenger aircraft flights outside the United States, its Territories and Canada, when coordinated by the Security Division and approved per reference (b), paragraph 9-12.

b. Secret. Transmit or transport Secret material by:

(1) Utilizing STE terminals authorized for, as a minimum, Secret transmission.

(2) Any of the means approved for the transmission of Top Secret except that Secret information may be introduced into the Defense Courier Service only when United States control of the information cannot otherwise be maintained. This restriction on use of the Defense Courier Service does not apply to SCI and COMSEC material.

(3) U. S. Postal Service (USPS) Registered Mail within and between the United States and its Territories.

(4) USPS Priority Mail Service may be used between command activities and other DoD activities within the United States and its Territories.

(5) USPS Registered Mail through Army, Navy, or Air Force postal service facilities, outside the United States and its Territories, provided the mail does not pass through a foreign postal system or any foreign inspection or via foreign airlines. The material must remain under U. S. Government control. Special care will be taken when sending classified material to U. S.

activities overseas. When in doubt, contact the Security Division to determine whether the material should be mailed.

(6) Authorized overnight domestic express delivery service (limited to CONUS delivery only). Use of street-side collection boxes and weekend deliveries is prohibited.

c. Confidential. Transmit or transport Confidential material by:

(1) Utilizing STE terminals authorized for, as a minimum, confidential transmission.

(2) Any means approved for the transmission of Secret information; however, use of the USPS for Confidential information is governed by the following: USPS Registered Mail will be used to and from FPO and APO addressees located outside the United States and its Territories and for NATO Confidential.

(3) USPS First Class mail will be used between command activities and any other DoD activities anywhere in the United States and its Territories. USPS First Class mail may not be used between command activities and non-DOD activities or contractors.

(4) Certified or Registered mail must be used when sending Confidential mail to the Department of State for forwarding by diplomatic pouch.

d. For Official Use Only (FOUO). FOUO documents and material may be transmitted via First Class mail, parcel post, or for bulk shipments, fourth-class mail. Fax or e-mail transmission of FOUO information (voice, data or facsimile) should be by encrypted communications systems whenever practical. FOUO information may be placed on DoD web sites with appropriate protective measures in place.

e. SCI and SAP Material. Transmit and transport SCI and SAP material by approved means as authorized by the SSO or the SAP manager respectively.

f. Receipt System

(1) Include a receipt, to be filled out and returned by recipients, when transmitting or transporting classified material above confidential outside the command. Failure to sign and return a receipt may result in a report of possible compromise.

(a) The sender will attach the receipt to the inner cover of the material being transmitted or transported. Prepare the inner cover as outlined in section 36-15g below. Use OPNAV Form 5511/10, Record of Receipt. OPNAV Form 5511/10 will be unclassified and contain only the information necessary to identify the material being transmitted. Prepare the outer cover as outlined in section 36-15g below, but do not seal it.

(b) Hand-carry the envelope/package to a second person to conduct a quality check prior to transmission. The following personnel are authorized to conduct quality checks: ASAC,

RAC, FOSO, security coordinator, PSA, others as identified by the DAD or SAC. The sender will retain a suspense copy of OPNAV Form 5511/10 and seal the outer cover.

(c) The sender will initiate tracer action when a signed receipt is not returned from the addressee within 30 days. Notify the appropriate security office when tracer action is initiated.

(d) Signed OPNAV Form 5511/10 will be retained for two years by the code or field office that forwarded the material.

(2) Receipts for confidential material are not required, except when transmitted to a foreign government (including embassies located in the United States).

g. Preparation of Classified Material for Transmission

(1) Properly prepare classified material for transmission to protect it from unauthorized disclosure.

(2) When classified material is transmitted, enclose it in two opaque, sealed envelopes or similar wrapping, as follows:

(a) Wrap, fold or pack written classified material so the text will not be in direct contact with the inner envelope or container. It may be necessary to fold the material if it has no cover.

(b) The inner envelope or container will show the address of the receiving activity, and the highest classification of the material enclosed including, where appropriate, “Restricted Data” markings and any special instructions. Carefully seal the envelope to minimize the possibility of access without leaving evidence of tampering. Attach the receipt to the inner envelope.

(c) When classified material is hand carried outside the command, a locked briefcase may serve as the outer wrapper or cover. If the briefcase will not lock, use a second opaque envelope as the outer wrapper.

(d) Do not place classification markings, listing of the classified contents, or any other unusual data or marks which might invite special attention to the fact that the contents are classified, on the outer cover. Mark the outer cover of Confidential material being transmitted by USPS First Class mail, “Postmaster: Do Not Forward, Return to Sender,” and “FIRST CLASS” or, for mail weighing over 12 ounces, “PRIORITY MAIL.”

h. Addressing

(1) Address classified material to another activity or official government agency, not to an individual. Office numbers or phrases in the address, such as “Attention: Records Department,” or similar aids in expediting internal routine delivery, in addition to the organization address, may be used. When it is considered appropriate to direct classified

material to the attention of an individual, the identity of the intended recipient should be indicated on an attention line on the inner container or in the letter of transmittal, not on the outer envelope.

(2) Show the address of the receiving activity on the inner envelope or container.

(3) Show the complete address of the recipient and the return address of the sender on the outer envelope or container.

i. Hand-Carrying Classified Within NCIS Facilities and on Military Installations

(1) When classified material is being carried within NCIS facilities or between buildings of the local military installation, the individual carrying the material will take reasonable precautions to prevent inadvertent disclosure.

(2) Within NCIS facilities, use coversheets, file folders or pouches to protect against casual observation of the classified information. Do not expose, view or read classified material in elevators, hallways, or any common areas.

(3) When carried between buildings on local installations, the courier must place a cover sheet on the classified material or seal the classified material in an opaque envelope bearing the classification markings appropriate for the material within. In addition, place the classified material in a locked briefcase or other suitable container that bears no outside classification markings. This will ensure that no undue attention is drawn to the courier.

(4) Hand-carry classified material off local installations as specified in section 36-14(j) below.

j. Authorization to Hand-Carry Classified Material in a Travel Status

(1) Hand-carrying of classified material in a travel status will be authorized only when classified material:

(a) Cannot be transmitted by other authorized means due to time constraints;

(b) Is required at the traveler's destination; and

(c) Is not available at the command to be visited.

(2) The Security Division or security coordinator will issue appropriate courier cards to those personnel who must hand-carry classified material in a travel status to or from NCIS facilities on a frequent basis (see section 36-14(k) below). The Security Division or appropriate security coordinator will brief each individual authorized to hand-carry classified material. Authorized individuals must also sign a statement acknowledging that they understood the briefing. This statement will be retained for a minimum of two years and need not be executed

on each occasion that the individual is authorized to transport classified information provided a signed statement is on file.

(3) When carried off the local installation, couriers must seal classified material in an opaque envelope bearing the classification markings appropriate for the material within. Place the classified material in a locked briefcase or other suitable container that bears no outside classification markings (see section 36-14(g)).

k. Hand-Carrying Classified Material on Commercial Passenger Aircraft

(1) Due to the possibility of hijacking, personnel are only authorized to hand-carry classified material aboard commercial passenger aircraft when other methods will not transmit the material in time to meet operational objectives.

(2) Approval to hand-carry classified material on commercial passenger aircraft is authorized. The Security Division, DAD or SAC will provide each individual carrying classified material aboard a commercial passenger aircraft, a written statement authorizing the transmission. This authorization statement, when possible, should be included in official travel orders and will ordinarily permit the individual to pass through security or customs control points without the classified material being subjected to inspection.

(3) Personnel will adhere to documentation requirements and procedures for carrying classified material aboard commercial passenger aircraft as outlined in reference (b), paragraph 9-10.

l. Issuance, Use and Control of Courier Cards

(1) The Security Division or security coordinator will issue courier cards to personnel who frequently hand-carry classified information to or from NCIS.

(2) Make requests for courier cards in writing to the Security Division or Security Coordinator through the cognizant DAD or SAC. Requests for courier cards must include a justification statement.

(3) The Security Division or security coordinator will issue DD Form 2501 to personnel after sufficient justification has been provided to indicate that the normal duties of the individual necessitate hand-carrying classified material on a routine or frequent basis. In this case, DD Form 2501 may be issued for a maximum period of two years.

(a) The security coordinator for each field office will keep an inventory/issue log to reflect the current status of all DD Form 2501 courier cards for their respective office. Security Division personnel will review field office courier logs during inspections and SAVs.

(b) The Security Division will keep an inventory/issue log to reflect the current status of all DD Form 2501 courier cards issued to headquarters personnel. The Security Division will maintain the log in TWMS.

(4) Bearer Courier Cards. NCIS does not authorize the issuance of "bearer" courier cards. Bearer courier cards do not contain the name of the person transporting the classified information. References (b) and (d) require that responsible officials identify personnel authorized to escort or transport classified material. The use of "bearer" courier cards does not meet the intent of this policy.

m. Telephone Transmission

(1) Do not discuss or transmit classified information over the telephone except via secure means such as secure telephone equipment (STE) terminals.

(2) In all other circumstances, the telephone system is not secure and any discussion of classified information or "talking around" classified information is prohibited.

(3) The use of speaker phones in areas where SAP and SCI is processed is prohibited. Disable the speaker function on all phones with such capabilities. In all other areas where classified information is processed, personnel must practice the need-to-know principle when using speaker phones for classified discussions.

n. Use of Secure Telephone Equipment (STE) Terminals

(b)(7)(E)

(2) See section 36-16 for guidance on contractor personnel requiring access to secure voice assets and COMSEC equipment.

(3) Prior to issue, users must complete a Responsibility Acknowledgement Form to be filed with the Electronic Key Management Systems (EKMS) manager that enumerates individual responsibilities of the user while the (b)(7)(E) is issued to the user. The user must provide the (b)(7)(E) to the EKMS manager in June and December to facilitate mandatory semiannual inventory. The (b)(7)(E) is not to be left in the STE terminal when not in use. If the (b)(7)(E) is to be stored in the same office space as the STE, it must be in a GSA-approved security container. If the (b)(7)(E) is to be stored in an office separate from the STE, it can be stored in a desk drawer.

(4) If a STE is installed within a SCIF, speaker phones must remain disabled.

o. Residential Use of Omni Devices

(1) The Security Division must approve installation and utilization of Omni Devices in private residences. Direct each request for approval to the Security Division. Upon approval,

the Security Division will forward the request to the EKMS manager. The EKMS manager will ensure the Omni Device has been prepared for residential use. The residential user will install the Omni Device in their respective residence. The EKMS manager will provide guidance on installation.

(2) Upon approval, the individual who is being issued the Omni Device will execute a responsibility statement outlining the user's responsibilities, identifying the residence by address and telephone number and establishing the requirement to physically deliver the Omni Device to the EKMS manager in June and December of each year for semiannual inventory. Failure to do so will result in revocation of residential Omni Device privileges. Retain a copy of the signed responsibility statement and return the original to the EKMS manager.

(3) Local custody issue may not exceed the tour length or period of assignment for which an individual requires the use of an Omni Device in the private residence. The Security Division will make contact with each residential Omni Device user annually, to ensure the requirement remains the same or to initiate return of the Omni Device.

(4) All installations should be considered temporary in nature and limited to key personnel who have an operationally driven requirement for after-hours discussion of sensitive/classified information. Only the person for whom it was installed shall use the residential Omni Device. When the residential Omni Device is no longer required in a residence, the user will return the Omni Device to the EKMS manager.

(5) The user must ensure the terminal is in a 'locked' condition following each use and retain the operational PIN within a properly prepared SF-700. Visually inspect the SF-700 monthly for signs of tampering and send an email to the EKMS manager each month stating the visual inspection has been conducted. Failure to do so will result in revocation of residential Omni Device privileges. Do not allow any sensitive or classified discussions to be overheard by other individuals within the residence.

(6) The authorized user is responsible for complying with all required security procedures and for preventing unauthorized access to a keyed device or any sensitive U.S. Government information that may be transmitted over that device. Notify the Security Division immediately if the Omni Device is tampered with or lost.

36-16. Storage and Destruction

a. Storage Requirements

(1) All classified material will be stored in a GSA-approved security container or a facility approved for storage of classified information.

(2) Store FOUO material in a manner that provides reasonable assurance that unauthorized persons do not gain access. During working hours, take reasonable steps to minimize risk of access by unauthorized personnel. After working hours, store FOUO, at a minimum, in a locked desk, file cabinet, bookcase, locked room or similar space.

b. Approval of Facilities. The NCIS Security Manager will approve NCIS facilities to process classified information. The Information Technology Directorate will only provide access to classified networks with the appropriate physical security accreditation. The following types of facilities will be approved to process classified information:

(b)(7)(E)

(2) A restricted access area (RAA) must meet physical requirements of reference (k), requires a letter from the DAD/SAC requesting restricted access area approval, and accreditation from the Security Manager. RAA also requires a certified protected distribution system (PDS) per reference (j).

(3) A controlled access area (CAA) must meet physical requirements of reference (k), requires a letter from the DAD/SAC requesting controlled access area approval, and accreditation from the Security Manager. CAA may require a certified PDS per reference (k).

(4) A secure room (secret open storage) must meet physical requirement of reference (b) Chapter 10, requires a letter from the DAD/SAC requesting open storage approval, and accreditation from the Security Manager.

(5) A Sensitive Compartmented Information Facility (SCIF) must meet physical requirements of reference (l), requires a letter from the DAD/SAC requesting a SCIF and requires accreditation from the Defense Intelligence Agency (DIA).

(6) A Special Access Program Facility (SAP-F) must meet physical requirements of reference (m), requires a letter from the DAD/SAC requesting a SAP-F, and requires accreditation from the SAP Security Manager.

c. Requesting Approval. The procedure for requesting approval to process classified information, or upgrading a previously designated facility to process classified at a higher classification, is comprised of two steps. A facility project request per reference (n), and a technology capability request per reference (o).

d. Intrusion detection systems (IDS). IDS will be installed in areas to protect classified information per reference (b). The IDS will be tested semi-annually and the results recorded on the NCIS Intrusion Detection Equipment Test Record.

e. Security Container and Cipher Lock Combinations

(1) Only personnel authorized by the Security Division or security coordinator can change combinations to security containers and cipher locks.

(2) Give combinations only to those personnel whose official duties require access to the security container.

(3) Change combinations when security containers are first placed in use and when any of the following occur:

(a) An individual knowing the combination no longer requires access; unless other sufficient controls exist to prevent that individual's access to the room or security container.

(b) The combination has been subject to possible compromise or the security container has been discovered unlocked and unattended; and

(c) The security container is taken out of service. Reset built-in combination locks to the standard combination (b)(7)(E)

(4) In selecting combination numbers, do not use sequential numbers (i.e., multiples of five, simple ascending or descending arithmetical series) and personal data, such as birth dates and Social Security numbers.

(5) Do not use the same combination for more than one security container in any one location.

(6) Seal records of combinations in the envelope portion of SF 700.

(a) Part 1 of SF 700 is the portion that is posted inside the main entrance door of facilities where classified information is processed, or inside the locking drawer of secure containers. Do not place any classification markings on Part 1 of the SF 700; it is not classified. However, it does contain personally identifiable information (PII) that shall be protected per reference (d), Volume 3.

(b) Mark Part 2 of the SF 700 with the highest level of classification authorized for storage in the room or container. Also, add the following statement to the bottom of Part 2, "Derived From: 32CFR 2001.80(d) (3);" and "Declassify on: Upon change of combination." See Figure 10-1 for a sample SF 700.

(c) Headquarters personnel will hand-carry the SF 700 envelopes to the Security Division. Personnel at main field offices and subordinate units must contact their security coordinator for retention instructions.

(7) Procurement, Transfer and Repair of Security Containers and Security Equipment

(a) Security equipment may be defined as locks, shredders, intrusion detection devices, secure facsimile machines or other related equipment. Contact your security coordinator for guidance on purchasing security equipment.

(b) Headquarters security coordinators will inform the Security Division when transferring security containers or other security equipment, from one area to another. Field office personnel should contact their local security coordinators.

(c) Security coordinators will notify the Security Division immediately to report problems with security containers or security equipment. The Security Division or security coordinator will coordinate all repairs of security containers and security equipment.

f. Destruction Procedures

(1) Destroy classified materials by utilizing only approved methods, such as shredding or burning.

(2) Only shredders approved by the National Security Agency (NSA) may be used to destroy classified material. Reference (p) is a list of NSA-approved shredders.

(3) The only authorized method to destroy classified and sensitive material at the RKB is by shredding. Burn bags are not authorized for storage or destruction at the RKB.

(4) For those field offices using other destruction methods because they do not have access to their own shredding machine, the following applies:

(a) When placed in service, boldly mark the front and back of all burn bags to reflect the highest classification of the contents, owner's name, office of origin, room number, telephone number, and date. Close burn bags securely with duct tape or staples.

(b) The weight of burn bags should not exceed 10 pounds. Burn bag facilities traditionally will not accept burn bags that are torn or damaged. Label burn bags containing material that cannot be shredded, such as classified plastic binders, classified photo negatives, etc., “BURN ONLY.”

(c) Only personnel who have a clearance equal to or above the classification of the material being destroyed are authorized to deliver burn bags to destruction facilities.

(5) The destruction of all Top Secret material shall be accomplished by two appropriately cleared persons. Complete OPNAV Form 5511/12, Classified Material Destruction Report, prior to carrying out destruction procedures for Top Secret material. This destruction record shall be maintained by the TSCO/TSCA for a period of five years.

(6) Reference (q) contains procedures used for declassifying or clearing automated information systems (AIS) media.

36-17. Industrial Security

a. The COR must notify the Security Division when contracts that include access to classified information or facilities where classified information is processed are being contemplated. Reference (r) requires that a DD Form 254, DoD Contract Security Classification Specification, be incorporated into each contract requiring access to classified information or facilities.

b. Each COR is responsible for providing the Security Division with the following items:

(1) Statement of Work or Performance Work Statement.

(2) Intelligence-Related Contracting Coordination Office (IRCCO) Checklist (for SCI contracts only).

(3) Copy of the Contract.

(4) List of company personnel who will be participating on the contract. This list must include their DoD Electronic Data Interchange (EDI) Personal Identifier (PN) or Social Security numbers, if DoD EDI PN is not available. CORs must provide an updated list of contractors each time there is an addition or deletion.

(5) Each COR must also coordinate with the company to provide clearance verification, via the Joint Personnel Adjudication System (JPAS), for all personnel working on the contract. The Security Division will accept clearance verification letters, in lieu of JPAS notifications, only when JPAS is unavailable.

c. Security Division personnel will take the following actions when notified that a contract is being awarded or an option year is being exercised:

(1) Review the Statement of Work or Performance Work Statement and the contract for accuracy. In addition, they will ensure that the documents contain appropriate classification requirements. This review also provides verification that contract employees will require access to classified information or some other aspect of the work is otherwise classified.

(2) Check the company's facility clearance in the Industrial Security Facilities Database.

(3) Prepare DD Form 254 in coordination with the following offices, as necessary:

(a) Representatives from the responsible headquarters code or field office (usually the COR will be one of the representatives)

(b) Acquisition and Logistics (Code 11B),

(c) Code 15,

1. Communications Security (COMSEC) Custodian.

2. Information Assurance Manager.

(d) Other as required,

(4) Keep copies of all documentation related to the contract for future reference.

(5) Create a Personnel Security File folder for each contractor indoctrinated for SCI.

(6) Process requests for access to NCIS facilities. Each request must be validated by the COR. The Security Division will issue appropriate badges to contractors requiring access to the headquarters facilities at the RKB. Contact your security coordinator for access procedures at field offices.

36-18. Security Incidents

a. Per reference (d), Volume 3, Enclosure (6), and reference (b), Chapter 12, this policy establishes standards and procedures for identifying, reporting, and conducting inquiries and investigations involving security incidents.

(1) Any NCIS individual who becomes aware that classified information may be lost or compromised will immediately notify the Security Division by the most expeditious means possible. Concurrently, the individual discovering this information should also advise their security coordinator and chain of command. Up to this point, the discovery is considered a security incident until the facts are obtained through a preliminary inquiry.

(2) Upon discovering classified information adrift or unprotected, the primary responsibility of the discoverer is to regain custody of the information and secure it in an approved security container as soon as possible.

b. There are two types of security incidents:

(1) Infraction. An infraction is a security incident involving failure to comply with requirements (i.e., the provisions of references (b) and (d), this Manual or other applicable security policy) which cannot reasonably be expected to, and does not, result in the loss, suspected compromise, or compromise of classified information. An infraction may be unintentional or inadvertent. While it does not constitute a security violation, if left uncorrected, can lead to security violations or compromises. It requires an inquiry to facilitate immediate corrective action but does not require an in-depth investigation.

(2) Violation. A violation is a more serious security incident that results in, or could be expected to result in, the loss, suspected compromise or confirmed compromise of classified information.

c. Inquiries

(1) Each office that generates a security incident will conduct a preliminary inquiry (PI) when classified information has been lost, compromised or subjected to possible compromise.

(2) The Security Division will coordinate with the DAD or SAC of the office generating the security incident to appoint a disinterested individual to serve as preliminary inquiry officer (PIO) to conduct the PI.

(3) The PIO will complete the PI within 72 hours of appointment and will follow the guidelines found in reference (b), paragraph 12-4.

(4) The PIO will send the completed PI report to the Security Division.

(5) The Security Division will evaluate the PI report and create a closeout memorandum. The Security Division will package the closeout letter, PI report and any other pertinent documents together and send the package to the DAD or SAC and other offices, as appropriate.

(6) The Security Division will make appropriate notifications upon conclusion of the PI as required by reference (b), Chapter 12.

(7) The closeout letter generated by the Security Division may include guidance for personnel to follow to preclude repeat security incidents. This guidance may include reading portions of appropriate security regulations, on-line training, or other corrective actions.

(8) The Security Division may also report results of PIs to the DoD Central Adjudication Facility as part of the Continuous Evaluation Program or Security Assessment and Evaluation Report system. The Security Division will notify individuals involved, along with their supervisor and DADs or SACs, if this course of action is taken.

(9) Supervisors may also want to take appropriate corrective or disciplinary action. Any action taken by the supervisor is in addition to actions taken by the Security Division.

d. Investigations

(1) When the circumstances of an incident require a more detailed examination, the Security Manager may request an investigation by the NCIS Inspector General, a headquarters department, a field office, or other appropriate agency.

(2) Judge Advocate General Manual (JAGMAN) Investigations

(a) Per reference (b), paragraphs 12-9 and 12-10, and reference (s), NCIS conducts JAGMAN investigations when compromise is suspected and one or more of the following are found during the preliminary inquiry:

1. The probability of harm to the national security cannot be discounted.

2. Significant security weaknesses have been revealed.

3. When punitive action is contemplated.

(b) The Inspector General, Code 00I, may elect to initiate an internal personnel inquiry on matters not sufficiently resolved by a JAGMAN investigation and when circumstances warrant such action.

e. Special Security Incidents. Reference (b), paragraph 12-8 provides specific information and guidance on matters related to special security incidents.

f. Practices Dangerous to Security

(1) Report deviances of security regulations, which do not result in a compromise or possible compromise, to the Security Division immediately upon discovery.

(2) The Security Division may act upon such reports and take corrective action, as needed, to preclude reoccurrence of similar incidents.

g. Unsecured Security Containers

(1) When a security container or facility, in which classified material is stored, is found unlocked, in the absence of cleared personnel, the individual finding the container unlocked will notify the security container custodian identified on the SF 700, Security Container Information Form. This form is located on the inside of the locking drawer of the security container or just inside the main entrance of the facility. The person who makes the discovery will guard the container until the custodian responds.

(2) The responding custodian will inspect the unsecured classified material to determine, as best as possible, if classified material is missing. When it appears that classified material is missing, immediately notify the Security Division. If a determination is made that nothing is missing, report the incident to the Security Division during normal duty hours.

(3) If there is evidence that the combination to the security container or facility may have been compromised, change the combination as soon as possible.

h. Public Media Compromises

(1) A public media compromise is the unofficial release of DoD classified and controlled unclassified information (CUI) to the public, resulting in its unauthorized disclosure.

(2) When an individual becomes aware that classified or CUI is unofficially released to the public (i.e., newspaper, magazine, book, pamphlet, radio, television broadcast or INTERNET) they shall immediately notify the Security Division.

i. Improper Transmission. In the event a code or field office receives classified material showing evidence of improper handling, addressing, packaging, transmission, or transport, promptly notify the sending activity. Contact the security coordinator and Security Division for guidance. When making the notification, use OPNAV Form 5511/51 (Security Discrepancy Notice) per reference (b), paragraph 12-19. Forward a copy of the Security Discrepancy Notice to the Security Division for retention. Retain all copies of the Security Discrepancy Form for two years.

j. Spillages. A spillage is an improper transmission that occurs on an information technology system. Notify the IAM, in addition to the Security Division and the offending command, when a spillage occurs.

k. Other Threats to Security. All personnel, military and civilian, whether they have access to classified material or not, will immediately report to the Security Division any suspected acts of sabotage, espionage, deliberate compromise, or other possible threats to security.

36-19. Counterintelligence and Security Reporting Requirements

a. Employees will report requirements in this Chapter to the Security Division within 72 hours.

b. Anonymous reports can be made via phone at (b)(7)(E) Web at www.ncis.navy.mil or Text "NCIS "+ your tip info to CRIMES (274637).

c. Personnel Security Reporting Requirements. As a condition of continued access to classified information, you have an obligation to report the following to the NCIS Security Division:

(1) Foreign Travel. Personnel with access to classified information who plan unofficial foreign travel shall:

(a) Report anticipated foreign travel through their immediate supervisors and to the SSO or local SCI security official. Failure to report foreign travel may result in reevaluation of eligibility for continued SCI access.

(b) Obtain a defensive travel security briefing or a risk-of-capture briefing from your supporting security office prior to travel. Briefings provide situational concepts of threats that can be encountered, regardless of the country of intended travel. Threat situations shall include those from foreign intelligence services, terrorist or narcotics groups, or indigenous groups active in promoting insurgency, war, civil disturbance, or other acts of aggression when physical safety and security of personnel cannot be reasonably provided.

(c) Complete a Foreign Travel Questionnaire upon completion of travel.

(2) Contact with Foreign Nationals. Employees with access to classified information must protect themselves against cultivation and possible exploitation by foreign nationals who are or may be working for foreign intelligence services and to whom they might unwittingly provide sensitive or classified national security information.

(a) Persons with access to classified information have a continuing responsibility to report, within 72 hours, to their local SCI security official (or immediate supervisor if an SCI security official cannot be contacted within 72 hours) all contacts:

1. That are of a close, continuing personal association, characterized by ties of kinship, affection, or obligation with foreign nationals. Casual contacts and associations arising from living in a community normally need not be reported.

2. In which illegal or unauthorized access is sought to classified, sensitive, or proprietary information or technology, either within or outside the scope of the employee's official activities. Personnel should be skeptical of requests for information that go beyond the bounds of innocent curiosity or normal business inquiries.

3. With known or suspected intelligence officers from any country.

4. With, or invitations from, foreign government officials.

(b) Unless specifically approved by the appropriate Head of the Intelligence Community Element (HICE), designee, or SIO; DoD SCI-indoctrinated personnel shall not initiate contact with foreign government representatives, accept invitations to attend any official or social foreign function, or to extend reciprocal invitations. DoD personnel whose official duties require them to deal officially and socially with foreign nationals must limit their contact and association to the requirements of their duties.

(c) Defense Attaché System personnel and other personnel whose duties require regular official contact with foreign government representatives and other foreign nationals are exempt from the approval requirements and from reporting of foreign contacts directly associated with their duties, except as required by their agency’s regulations. The HICE, designee, or SIO may exempt other personnel, on a case-by-case basis, whose duties require regular contact with foreign nationals.

1. Defense Attaché System personnel and other personnel whose duties require regular contact with foreign government representatives and other foreign nationals are not exempt from the 72-hour reporting requirement whenever an incident occurs as described in paragraph 16.a. of this enclosure.

2. Based on the foreign contact report, the SSO or SCI security official may require the reporting individual to complete a foreign contact questionnaire. The SCI security official shall forward a copy to the local supporting CI activity for action and retain an information copy in the individual’s personnel security file. Discussions of any contact reports shall be restricted to those with a demonstrated need to know. Under no circumstances shall the individuals involved, their supervisor, or the local SCI security officer make any attempt to investigate such matters. Investigations of any contact reports shall be the responsibility of the appropriate CI activity.

(d) Failure to report foreign contacts as required above may result in reevaluation of eligibility for continued SCI access. This reporting requirement does not imply that an individual shall automatically be subject to administrative action if he or she reports questionable contacts or associations.

(3) Counseling. Employees will report psychological, mental or emotional counseling and counseling for personality disorders. Employees are not required to report consultations related to issues that are strictly marital or family related. In addition, employees are not required to report counseling related to adjustments from service in a military combat environment.

(4) Drug Use. Employees will report illegal or improper use of narcotics, non-medicinal drugs, non-prescription drugs or controlled substances.

(5) Personal Life Changes. Employees will report name changes, changes in marital status, and cohabitation status.

(6) Criminal Conduct. Employees will report all arrests, regardless if convicted or not.

(7) Alcohol Related Incidents. Employees will report arrests, professional treatment or counseling relating to alcohol dependency.

(8) Financial Concerns. Employees will report excessive indebtedness, liens on property, collections, garnishments, judgments and unexplained financial affluence.

(9) Improper Security Practices. Employees will report:

(a) Inadvertent or deliberate removal of classified information or materials to an unauthorized area.

(b) Inadvertent or deliberate unauthorized destruction of classified information or materials.

(c) Knowledge of a security violation or infraction committed by the individual or other personnel.

(d) Deliberate or inadvertent disclosure of classified information or materials to an unauthorized person.

(e) Loss of classified information or materials.

(f) Requests for classified or sensitive information or materials through unauthorized channels (e.g. unclassified information systems).

(10) Computer/AIS Systems Misuse. Employees will report the following:

(a) Unauthorized entry into an automated information system (AIS), whether government or contractor, for any reason.

(b) Modification, destruction or manipulation of hardware or software, whether government or contractor equipment.

(c) Password Misuse

1. Obtaining or using someone else's password to browse through another's account without permission.

2. Sharing a password.

3. Copying or deleting information from another's account without their permission.

d. All personnel will report the following activities to the Security Division:

(1) Known or suspected acts of sabotage, espionage, terrorism, subversion, or deliberate compromise.

(2) Suicide or attempted suicide by personnel who have access to classified information.

(3) Unauthorized absences of personnel who have access to classified information if the DAD or SAC determines that the absence may be contrary to the interests of national security.

(4) Death or desertion of personnel who have access to classified information if the DAD or SAC determines that unusual indicators or circumstances may have existed that may cause concern.

e. Reportable Foreign Intelligence Contacts, Activities, Indicators, and Behaviors. Personnel who fail to report the contacts, activities, indicators, and behaviors in items 1 through 22, below, are subject to punitive action per reference (t). The activities in items 23 and 24 are reportable, but failure to report these activities may not alone serve as the basis for punitive action.

(1) When not related to official duties, contact with anyone known or believed to have information of planned, attempted, actual, or suspected espionage, sabotage, subversion, or other intelligence activities against DoD facilities, organizations, personnel, or information systems. This includes contact through Social Networking Services that is not related to official duties.

(2) Contact with an individual who is known or suspected of being associated with a foreign intelligence or security organization.

(3) Visits to foreign diplomatic facilities that are unexplained or inconsistent with an individual's official duties.

(4) Acquiring, or permitting others to acquire, unauthorized access to classified or sensitive information systems.

(5) Attempts to obtain classified or sensitive information by an individual not authorized to receive such information.

(6) Persons attempting to obtain access to sensitive information inconsistent with their duty requirements.

(7) Attempting to expand access to classified information by volunteering for assignments or duties beyond the normal scope of responsibilities.

(8) Discovery of suspected listening or surveillance devices in classified or secure areas.

(9) Unauthorized possession or operation of cameras, recording devices, computers, and communication devices where classified information is handled or stored.

(10) Discussions of classified information over a non-secure communication device.

(11) Reading or discussing classified or sensitive information in a location where such activity is not permitted.

(12) Transmitting or transporting classified information by unsecured or unauthorized means.

(13) Removing or sending classified or sensitive material out of secured areas without proper authorization.

(14) Unauthorized storage of classified material, regardless of medium or location, to include unauthorized storage of classified material at home.

(15) Unauthorized copying, printing, faxing, e-mailing, or transmitting classified material.

(16) Improperly removing classification markings from documents or improperly changing classification markings on documents.

(17) Unwarranted work outside of normal duty hours.

(18) Attempts to entice co-workers into criminal situations that could lead to blackmail or extortion.

(19) Attempts to entice DoD personnel or contractors into situations that could place them in a compromising position.

(20) Attempts to place DoD personnel or contractors under obligation through special treatment, favors, gifts, or money.

(21) Requests for witness signatures certifying the destruction of classified information when the witness did not observe the destruction.

(22) Requests for DoD information that make an individual suspicious, to include suspicious or questionable requests over the internet or Social Networking Services.

(23) Trips to foreign countries that are:

(a) Short trips inconsistent with logical vacation travel or not part of official duties.

(b) Trips inconsistent with an individual's financial ability and official duties.

(24) Unexplained or undue affluence.

(a) Expensive purchases an individual's income does not logically support.

(b) Attempts to explain wealth by reference to inheritance, luck in gambling or a successful business venture.

(c) Sudden reversal of a bad financial situation or repayment of large debts.

f. Reportable International Terrorism Contacts, Activities, Indicators, and Behaviors. Personnel who fail to report the contacts, activities, indicators, and behaviors in items 1 through 9, below, are subject to punitive action per reference (t). The activity in item 10 is reportable, but failure to report this activity may not alone serve as the basis for punitive action.

(1) Advocating violence, the threat of violence, or the use of force to achieve goals on behalf of a known or suspected international terrorist organization.

(2) Advocating support for a known or suspected international terrorist organizations or objectives.

(3) Providing financial or other material support to a known or suspected international terrorist organization or to someone suspected of being an international terrorist.

(4) Procuring supplies and equipment, to include purchasing bomb making materials or obtaining information about the construction of explosives, on behalf of a known or suspected international terrorist organization.

(5) Contact, association, or connections to known or suspected international terrorists, including online, e-mail, and social networking contacts.

(6) Expressing an obligation to engage in violence in support of known or suspected international terrorism or inciting others to do the same.

(7) Any attempt to recruit personnel on behalf of a known or suspected international terrorist organization or for terrorist activities.

(8) Collecting intelligence, including information regarding installation security, on behalf of a known or suspected international terrorist organization.

(9) Familial ties, or other close associations, to known or suspected international terrorists or terrorist supporters.

(10) Repeated browsing or visiting known or suspected international terrorist websites that promote or advocate violence directed against the United States or U.S. forces, or that promote international terrorism or terrorist themes, without official sanction in the performance of duty.

g. Reportable Foreign Intelligence Entities (FIE)-Associated Cyberspace Contacts, Activities, Indicators, and Behaviors. Personnel who fail to report the contacts, activities, indicators, and behaviors in items 1 through 10, below, are subject to punitive action per reference (t). The indicators in items 11 through 19 are reportable, but failure to report these indicators may not alone serve as the basis for punitive action.

(1) Actual or attempted unauthorized access into U.S. automated information systems and unauthorized transmissions of classified or controlled unclassified information.

(2) Password cracking, key logging, encryption, steganography, privilege escalation, and account masquerading.

(3) Network spillage incidents or information compromise.

(4) Use of DoD account credentials by unauthorized parties.

(5) Tampering with or introducing unauthorized elements into information systems.

(6) Unauthorized downloads or uploads of sensitive data.

(7) Unauthorized use of Universal Serial Bus, removable media, or other transfer devices.

(8) Downloading or installing non-approved computer applications.

(9) Unauthorized network access.

(10) Unauthorized e-mail traffic to foreign destinations.

(11) Denial of service attacks or suspicious network communications failures.

(12) Excessive and abnormal intranet browsing, beyond the individual's duties and responsibilities, of internal file servers or other networked system contents.

(13) Any credible anomaly, finding, observation, or indicator associated with other activity or behavior that may also be an indicator of terrorism or espionage.

(14) Data exfiltrated to unauthorized domains.

(15) Unexplained storage of encrypted data.

(16) Unexplained user accounts.

(17) Hacking or cracking activities.

(18) Social engineering, electronic elicitation, e-mail spoofing or spear phishing.

(19) Malicious codes or blended threats such as viruses, worms, trojans, logic bombs, malware, spyware, or browser hijackers, especially those used for clandestine data exfiltration.

36-20. Personnel Security

a. Basic Policy and Authority. The NCIS Personnel Security Program (PSP) is governed by reference (c) and incorporates PSP policies and procedures established by other executive branch agencies.

b. Personnel Security Program. The objective of the PSP is to conduct initial and continuous access to classified information and/or initial and continued assignment to sensitive duties, for personnel assigned to NCIS.

(1) No individual assigned to NCIS will be given access to classified information or be assigned to sensitive duties unless a favorable personnel security determination has been made to determine their loyalty, reliability and trustworthiness. The initial determination will be based on a personnel security investigation (PSI) appropriate to the access required or to other considerations of the sensitivity of the duties assigned.

(2) Only the Security Division is authorized to request PSIs on NCIS personnel.

(3) The Security Division will not request investigations for civilian or military personnel who will retire, resign or separate with less than one year of service remaining.

c. Designation of Civilian Sensitive Positions

(1) SACs and DADs will conduct a position sensitivity review (PSR), when the position description is updated, to determine which of the following is applicable:

(a) Critical-sensitive.

(b) Special sensitive.

(c) Noncritical-sensitive.

(d) Non-sensitive.

(2) Utilize the criteria found in reference (c), Chapter 5.

(3) The PSR process is conducted by using the Office of Personnel Management (OPM) Position Designation Tool Worksheet. The Position Designation Tool Worksheet can be found at: http://www.opm.gov/investigate/resources/position/PosDesig-Step1.aspx.

d. Designation of Military Positions. The respective SAC or DAD will review each military position and designate a security access level for that position.

e. Sensitive Positions. The Security Division will review positions designated as sensitive to ensure that only those positions that meet the criteria in reference (c), Chapter 5, are designated as sensitive and that the number of positions designated as sensitive is held to the minimum consistent with mission requirements. The Personnel Security Program Manager will maintain records of sensitive positions by category and ensure the results are accurate in the Joint Personnel Adjudication System (JPAS).

36-21. Clearances and Sensitive Assignment Eligibility Determinations

a. Personnel Security Determination Authority. The Security Manager is assigned responsibilities as follows:

(1) Initiate personnel security investigations on agency personnel, when required.

(2) Request security clearance eligibility from the Department of Defense Central Adjudication Facility (DoD CAF) Navy Division, for all assigned personnel.

(3) When necessary, grant interim security clearances. Extend interim security clearances and notify DoD CAF, Navy Division when security clearance is not received in 180 days.

(4) Certify security clearance eligibility and access authorizations of members of the agency to other activities when required.

(5) Administratively upgrade or downgrade security clearances, as appropriate, based on a change to the position sensitivity, and notify DoD CAF, Navy Division of the action taken.

(6) Establish procedures to continuously evaluate members of the agency with regard to eligibility for access to classified information.

(7) Suspend individual access to classified information when warranted.

(8) Comply with administrative processing instructions contained in any Letter of Intent (LOI), Letter of Notification (LON) or Conditional Security Determination received from DoD CAF, Navy Division concerning NCIS personnel.

(9) Comply with instructions contained in written notifications from the Personnel Security Appeals Board regarding the final disposition of any security determination appeals made against agency personnel.

(10) Suspend access and notify DoD CAF, Navy Division when a civilian employee with a security clearance is incarcerated (to include work release programs) as the result of a conviction for a criminal offense or is absent without leave for a period exceeding 30 days.

(11) Suspend access and notify DoD CAF, Navy Division when a military member with a security clearance is adjudged a punitive discharge (dismissal, bad-conduct discharge or dishonorable discharge) by a court-martial, issued an other-than-honorable discharge via administrative separation proceedings, incarcerated (to include work release programs) as the result of a conviction for a criminal offense by court-martial or civilian court, or is declared a deserter.

b. Clearances and Personnel Security Determinations

(1) A personnel security clearance is an administrative determination that an individual is eligible for access to classified information at a specified level of classification. A security clearance is not de facto authorization for an individual to access classified information. Authorization to access classified information is a separate determination based on the individual's security clearance and need to access classified information in the performance of official duties.

(2) A security clearance may be authorized only for the level of access required to perform assigned duties.

(3) A Classified Information Nondisclosure Agreement (SF 312) must be executed by all personnel as a condition of access to classified information. Personnel who have previously executed an SF 189, SF 189-A or other nondisclosure agreement (NDA) allowed by the National Security Council (NSC), as provided in 32 CFR, Section 2003.20, need not execute a SF 312.

c. Security Clearance

(1) Security Clearance Granting Activity. A security clearance is granted upon favorable adjudication of all completed investigative requirements as set forth in reference (c), Chapter 8.

(2) Security Clearance Upgrade. When an individual requires a higher level of security clearance and the investigative basis supports the higher security clearance, the Security Division will submit a request to DoD CAF, Navy Division to upgrade the security clearance.

d. Unfavorable Determination Notification and Appeal Process

(1) An unfavorable personnel security determination may result when a review of derogatory information regarding an individual raises questions concerning trustworthiness or loyalty.

(2) The process involved in administering unfavorable determinations concerning security clearances is described in reference (c), Chapter 8. The Security Division will provide all LOIs and LONs to the employee and ensure that the recipient is afforded every reasonable opportunity to refute, mitigate, offer explanations and appeal determinations, as appropriate. The Security Manager will ensure that an appropriate agency endorsement is included on any correspondence forwarded to the proper adjudicative authority when required. The Security Division will forward all correspondence associated with subject's response to LOIs, LONs or appeals as appropriate.

e. Continuous Evaluation of Eligibility

(1) Each individual will be continuously evaluated regarding eligibility for access to classified information or service in a sensitive civilian position.

(2) All members of the agency must report any potentially significant information, which could place in question an individual's loyalty, reliability or trustworthiness. Any information that falls into the categories listed in Appendix G of reference (c), and paragraph 36-19 of this chapter will be reported to the Security Division for evaluation. Members of NCIS will not attempt to interpret or evaluate the significance of the information to determine whether to report.

f. Co-workers must advise their chain of command, security coordinator, and the Security Division when they become aware of information with potentially serious security significance regarding someone with access to classified information or employed in a sensitive position.

g. The Security Manager will make a determination, upon initial receipt of credible derogatory information, whether to suspend the individual's access to classified information and/or sensitive duties. The Security Division will report credible derogatory information to the DoD CAF, Navy Division. Direct contact by any NCIS personnel, other than from the Security Division, with DoD CAF, Navy Division or Navy SSO concerning any employee's continued eligibility to maintain a security clearance or special access is prohibited.

36-22. Unfavorable Eligibility Determinations and Restrictions

a. Administrative Withdrawal or Adjustment of Clearance

(1) The Security Manager will administratively downgrade or withdraw the security clearance of employees who fail to submit their request for periodic reinvestigation.

(2) The Security Manager will administratively withdraw an individual's security clearance when it is no longer required for the performance of official duties at NCIS. The Security Division (headquarters personnel) or security coordinator (personnel at field offices and subordinate units) will debrief the individual as outlined in reference (c), paragraph 4-11, and file the executed security termination statement in the individual's personnel security file.

(3) When the level of access required for an individual's official duties changes, the DAD or SAC must submit a new position designation tool worksheet to the Security Division to adjust the individual's level of security clearance accordingly. After favorable review of locally available records, the Security Division will submit a request for security clearance eligibility to DoD CAF, Navy Division.

b. Denial or Revocation of Security Clearance Eligibility for Cause

(1) In the event the DoD CAF, Navy Division determines that an individual either fails or ceases to meet the security determination criteria as set forth in reference (c), paragraph 7-4, the DoD CAF, Navy Division will deny or revoke the individual's security clearance and/or sensitive duty assignment eligibility.

(2) In cases where security clearance eligibility is revoked, the Security Division will debrief the individual per reference (c, paragraph 4-11, debrief security access from JPAS and file the executed Security Termination Statement in the individual's personnel security file.

36-23. Access

a. Granting Access. Access to classified or sensitive information may be granted to members who have an official need-to-know, a favorable security eligibility, and assignment to a sensitive position. Members must execute a Classified Information Non-disclosure Agreement (SF-312) prior to being granting access.

b. Temporary Access (Interim Clearance)

(1) The Security Division may grant temporary access, pending completion of full investigative requirements or revalidation of security clearance. When it is necessary to request temporary access, DADs or SACs will provide justification in writing to the Security Division.

(a) Temporary Access Based On a Completed Investigation. The Security Manager may grant temporary access for 180 days on the basis of a favorable National Agency Check with a Local Agency Check (NACLC) or Access National Agency Check with Investigation (ANACI). When temporary access is based on a background investigation that is older than five years, the Security Division will notify the subject to submit a periodic reinvestigation (PR) within 30 days. If a PR is not submitted within 30 days, temporary access will no longer be valid and will be administratively downgraded.

(b) Temporary Access Based On a Pending Investigation. The Security Manager may grant an interim Secret clearance for 180 days on the basis of a favorable review of local records; favorable review and submission of a NAC, ANACI, NACLC, or SSBI request, as appropriate.

(c) Upon Transfer from Another DON Command. The Security Manager may grant temporary access for 180 days on the basis of prior established security clearance eligibility, provided security clearance eligibility can be verified and a check of local records does not reveal unfavorable information.

(2) The Security Manager may extend temporary access beyond 180 days per reference (c), paragraph 9-4.

(3) The Security Division will record temporary accesses granted by the Security Manager in the JPAS.

(4) The Security Division will request new personnel security determinations on individuals whenever they are being considered for higher levels of security clearance than they currently hold.

c. Interns

(1) The Security Division will grant access to NCIS facilities, where no classified information is processed, to personnel participating in various intern programs. This facility access does not confer access to classified or sensitive information. The interns will be assigned to public trust positions after having a favorably adjudicated personnel security investigation.

(2) A more in-depth investigation is conducted for interns requiring access to classified information or facilities where classified information is processed.

d. Limited Access Authorization (LAA)

(1) LAAs are granted for non-U.S. citizens with unique skill sets and expertise, or who are supporting special projects. LAA is not authorization for access to classified information unless authorized by the Security Manager.

(2) Submit requests for LAA to the Security Division via the SAC. Include the following in the request package:

(a) Letter from SAC providing full justification.

(b) Single Scope Background Investigation (SSBI) via the OPM e-QIP.

(c) Set of Blue Applicant Fingerprint Cards.

(d) Foreign Disclosure Agreement Authorization from the NCIS Foreign Disclosure Officer.

(e) Letter from member indicating a willingness to undergo a Counterintelligence Scope Polygraph.

e. (b)(7)(E) The Security Division will grant access to (b)(7)(E) information, for personnel with a favorably adjudicated Single Scope Background Investigation, under the following conditions:

(1) Personnel in positions requiring access to (b)(7)(E) information.

(2) Personnel requiring access to the (b)(7)(E)

f. Termination of Access. Access will be terminated for members who no longer require it for the performance of their assigned duties and/or when the member's eligibility is suspended, denied or revoked.

36-24. Visitor Control

a. Classified Visits to NCIS

(1) A visitor is defined as any individual who is not assigned to the agency as active duty or reserve military, civilian employee or contractor. When escorts are used, they must make sure visitors have access only to information they have been authorized to receive. Some visitors may be permitted less restricted access to spaces based on certification of their security clearances and accesses.

(2) The Security Division will accept security clearances in conjunction with requests for access to classified information or facilities at the RKB. Security coordinators will use JPAS to verify visitor's clearances. Visitors who are not located in the JPAS will have to pass their clearances to the Security Division or security coordinator, as appropriate.

(3) The NCIS point of contact hosting the visitor is responsible for ensuring that information required in paragraph 36-24a(4) below is conveyed to the visitor to facilitate submission of the visit request to the Security Division or security coordinator. The NCIS point of contact is responsible for determining the visitor's "need-to-know," prior to granting access to any classified information, and to withhold classified information from the visitor when considered necessary.

(4) Visit requests can be sent through JPAS. If the sending agency does not have JPAS access, they may send the visit request in writing, by naval message, fax or mail. The following information is required:

(a) Full name, rank, rate, or grade (when applicable), SSN, title, position, and citizenship of the proposed visitor. If the visitor is an immigrant alien, this information must be indicated.

(b) Employer or sponsor, if other than the originator of the request.

(c) POC for visit, date, time and duration of the proposed visit.

(d) Detailed purpose of visit, when possible, including estimated degree of access required. When the visit involves access to special access program information, for which specific authorization is required, the visiting command must confirm that the visitor has been briefed and authorized such access.

(e) Security clearance status of visitor (the basis of clearance is not required).

(5) Submit requests for visits to other agencies at least five working days in advance of the proposed visit, in order to permit sufficient time for processing and to make a determination as to whether or not the visitor should or will be granted access. When a visit requirement comes up suddenly, furnish the above information by telephone to the Security Division. Personnel must follow-up last minute telephone requests by promptly submitting NCIS Form 5521/1to the Security Division. Message and e-mail visit requests must include all of the required information listed in paragraph 36-24a(4) above. Security Division personnel and security coordinators are not authorized to accept visit requests hand-carried by the visitor's themselves.

(6) To avoid any question of the legitimacy of the visit request, transmit submissions from security office to security office. An official, other than the visitor, with command signature authority, must sign the visit request.

(7) A visitor whose security clearance and access have been approved by the Security Division or security coordinator will be issued the appropriate badge or similar credential for the duration of the visit. Visitors displaying such credentials will not require escort in common areas and may move freely throughout the facility. However, entry into any restricted area or other area where classified information is being processed, open for view, is being discussed, or is otherwise accessible, will require an escort to preclude unauthorized access to such information. Do not grant access to classified information to visitors solely based on presentation of visitor badge.

b. Classified Visits by NCIS Personnel to Other Organizations. The Security Division is the sole authority permitted to certify clearances for classified visits by NCIS personnel to other organizations. Forward NCIS Form 5521/1, Security Clearance Request to the Security Division e-mail group at (b)(7)(E) @ncis.navy.mil.

c. Unclassified Visits to NCIS. Provide notification of visits that will not involve access to classified information (i.e., guest lecturers to the Training Department) to the Security Division or security coordinator at least five days prior to the visit.

d. Non-Official Visits To NCIS. Keep non-official visits to a minimum. Approval from the Security Division, for unofficial visits to the RKB or SAC, for unofficial visits to field offices and subordinate units is required. Upon approval, the following will apply:

(1) Submit names of visitors to the Security Division or security coordinator at least five days prior to the visit.

(2) Visitors will wear "Escort Required" badges or similar credentials, while within the perimeter. Children under 12 years of age are not required to wear a badge or credentials.

(3) Sponsors will provide escorts and ensure that all non-official visitors are escorted at all times.

(4) Non-official visitors may enter only unclassified areas of NCIS facilities other than areas approved by the Director or SAC for the visit.

(5) Adults shall accompany minors (under 12 years) at all times.

36-25. Foreign Visit Requests and Sponsorships

a. Basic Policy. This section establishes roles, responsibilities, and procedures for processing requests for foreign national visits and executive level engagement to NCIS facilities per references (b), (d), (r) and (u) through (x). Procedures identified in this section will help NCIS employees determine what information is needed to properly address national disclosure policy, physical security, protocol, and Foreign Visit System (FVS) reporting requirements. This section also establishes the process which ensures that requesting foreign national governments provide security assurance for individuals when classified information is involved during the visit, and facilitates visit logistics to include the date, time, and place of the visit. Definitions regarding key terms are provided in Appendix (E).

(1) Foreign nationals requesting to visit NCIS facilities inside the United States shall submit their request through their government embassy located in Washington, D.C. Visits by foreign nationals to NCIS facilities will be processed through the FVS.

(2) Foreign nationals requesting to visit NCIS facilities outside the United States will submit their visit request directly to the responsible SAC. Embassies in Washington D.C. will not process visit requests for visits outside the United States. SACs outside the United States may approve foreign visits to facilities where classified information is processed at the secret level or below. SACs must follow approval and operational procedures found in paragraph 36-25c for visits to SCIFs in overseas locations. Additionally, NCIS personnel will follow all procedures pertaining to foreign national visitors if the visit is to a facility where classified or sensitive information is processed.

(3) Visits by foreign nationals shall be arranged under the procedures for a one-time visit, a recurring visit, or an extended visit described in the Foreign Visit Request Flowchart provided at Appendix (D).

(4) Foreign national visits to NCIS facilities shall be controlled to ensure foreign nationals are not permitted unauthorized access to classified or sensitive information.

(5) This policy does not apply to visits to NCIS facilities by foreign national employees of U.S. contractors owned by foreign interests; these visits will be processed per guidelines provided by reference (v).

b. Responsibilities

(1) A foreign national visit request shall be initiated and signed by a SAC or DAD or above (or military equivalent personnel) and submitted to the Security Division for coordination and approval using the Foreign Visit Request Form 5512/5.

(2) The NCIS headquarters office code or field office sponsor shall:

(a) Inform the foreign national requesting a visit to an NCIS facility to contact their local embassy in Washington, D.C. to establish sponsorship;

(b) Forward a signed foreign visit request (NCIS Form 5512/5) to the Security Division 30 calendar days prior to the proposed visit. Exceptions are granted on a case-by-case basis by the Security Manager;

(c) Designate an NCIS government employee to escort and to control the activities of foreign nationals during the visit. Unescorted access within NCIS facilities by foreign national visitors is not allowed;

(d) Forward all information to be presented to foreign nationals to the NCIS foreign disclosure officer (Code 25) for review no less than 14 days prior to the visit. Identify foreign nationals as such when dealing with others through oral, written, and electronic communications;

(e) Ensure foreign nationals are provided access only to information which has been authorized for release to their government and which is necessary to fulfill the terms of their authorized certification;

(f) Ensure foreign nationals are not permitted access to automated information systems unless the systems have been sanitized or configured to ensure that foreign nationals' access to information is limited to that which has been authorized for release to their government. In no case shall a foreign national have unsupervised access to automated information systems regardless of his or her security assurance; and

(g) If the Security Manager does not concur with the foreign visit request, and the NCIS office code or field office sponsor has justifiable reasons for the visit to occur, the request may be resubmitted to the Principle Executive Assistant Director for Management and Administration for a decision.

(3) The Security Manager or appointed designee shall:

(a) Coordinate foreign national visits with the foreign disclosure officer, the appropriate desk within the Directorate of Intelligence and Information Sharing (DIIS), Strategic

Initiatives Office, and the Communications Directorate within 48 hours of receipt of the formal request to visit NCIS facilities are submitted;

(b) Review and make a decision to concur or not concur with the foreign national visit request;

(c) Notify the NCIS sponsor of the decision regarding the foreign national visit request;

(d) Process and record in the FVS, decisions made regarding the visit by foreign nationals involving access to classified and controlled unclassified information;

(e) Monitor the FVS and notify the NCIS sponsor of the approved or disapproved sponsorship of the foreign national visit by the appropriate embassy; and

(f) Notify the appropriate NCIS headquarters office code or field office security coordinator of the approved foreign national's visit, date, time, badge requirements, and the NCIS headquarters office code or field office sponsor or escort's name and telephone number.

(4) The DIIS and the Communications Directorate shall:

(a) Coordinate all matters of protocol to include the determination of VIP status and the level of engagement;

(b) Coordinate foreign national visits with the U.S. Department of State;

(c) Manage the Executive Engagement Tracking Database;

(d) Coordinate pre-briefs and, or background information for NCIS senior leadership, or

(e) Ensure the foreign visit complies with established NCIS international engagement strategy.

(5) The foreign disclosure officer will review and approve all information that will be disclosed or released to foreign nationals including but not limited to: briefings, slides, documents, talking points and products.

c. Procedures

(1) There are three types of visit authorizations:

(a) A one-time visit authorization which permits contact by a foreign national with a DoD component or DoD contractor facility for a single, short-term occasion (normally less than 30 days) for a specified purpose;

(b) A recurring visit authorization permits intermittent visits by a foreign national to a DoD component or DoD contractor facility over a specified period of time for a government approved license, contract agreement, or other program when the information to be released has been defined and approved for release in advance by the U.S. Government; and

(c) An extended visit authorization permits a single visit by a foreign national for an extended period of time. Extended visit authorizations are to be used when foreign nationals are required to be in continuous contact with a DoD component or a DoD contractor facility beyond 30 days for one of the following situations:

1. A foreign government contract or joint program (e.g., joint venture, representative to a joint multinational program);

2. Foreign liaison officer assigned or certified to a DoD component;

3. Participation in the Defense Personnel Exchange Program;

4. Cooperative Program Personnel assigned to a DoD component; or

5. Training, except those individuals on Invitational Travel Orders.

(2) Any SAC or DAD and above or military equivalent personnel may sponsor and submit foreign national visit requests on behalf of his or her NCIS code or field office. A foreign visit request must be submitted as far in advance as possible, but not less than 30 days prior to the proposed foreign national visit to enable adequate coordination with the appropriate embassy located in Washington, D.C. A form fill soft copy of NCIS Form 5512.5 is available in Lighthouse.

(3) If the Security Manager concurs with the foreign visit request, the approval will be sent to the appropriate embassy through the FVS. If the Security Manager does not concur with the foreign national visit request, the NCIS code or field office sponsor will be notified of the non-concurrence and basis of the decision. If the NCIS code or field office sponsor chooses, he or she may appeal the non-concurrence per paragraph 36-25b(2)(g).

(4) The Security Division will coordinate with the appropriate NCIS code or field office security coordinators on all approved foreign national visit requests and update the FVS with current and relevant information.

(5) Access to SCIFs by foreign nationals is prohibited unless approved in writing by the Director or designee on the operational need. Foreign national access to SCIFs for an open house, tour, orientation visit, or similar activity is prohibited unless approved by the Director of Naval Intelligence, or his designee.

(6) SCIF personnel will maintain a low profile of SCIF functions and activities to preclude expectations or requests for unauthorized access to information. The following procedures apply:

(a) Keep the number of foreign nationals in SCIF areas to a minimum;

(b) Sanitize the SCIF and brief all SCIF personnel prior to the entrance of foreign national visitors. Do not conduct or discuss SCI or mission business during the visit. The existence of covert, SAP, or other sensitive operations in the facility must not be exposed or otherwise acknowledged to the individual;

(c) Do not permit cameras, cellular phones, recorders, or other prohibited items in the SCIF; and

(d) Record the names of the visitor(s) in the SCIF visitor's log.

36-26. Access to the Joint Personnel Adjudication System (JPAS)

a. The Security Division will ensure all employee clearance information is recorded in JPAS, reflecting access determinations; which include temporary access, upgrades, downgrades, and suspensions. Additionally, NCIS must document interim security clearance determinations, execution of the Classified Information Nondisclosure Agreements (SF 312), and personal attestations in JPAS. JPAS is also used to submit continuous evaluation reports, pass visit requests, determine security clearance and SCI access eligibility, determine status of requested personnel security investigations and request DoD CAF, Navy Division adjudications. These inputs are accomplished by the Security Division.

b. Field offices and headquarters codes use JPAS to confirm the results of polygraphs, determine clearance status for subjects of investigations and to obtain information that might aid in other law enforcement operations. Therefore, each field office and code is authorized to designate JPAS account holders based on the size of the office, number of subordinate offices, operational responsibilities and support to the agency.

(1) Appendix (C) lists the number of authorized personnel for each code and field office. All authorizations are based on personnel occupying the following positions: field office support officers (FOSOs), supervisory management analysts, office managers, program support assistants, desk officers, Multiple Threat Alert Center personnel, STAAT PAC or LANT security training personnel, special security representatives and security coordinators. Requests by field offices and codes to modify authorizations will be considered on a case-by-case basis.

(2) The Security Division will give authorized users Level 7 or Level 8 (determined by type of Investigation) authority, which grants read-only access to the database, unless otherwise authorized.

(3) Field offices and codes must notify the Security Division when account holders no longer require access to JPAS. A replacement can be identified at that time. If no replacement for the former account holder is identified, the spot will remain unfilled until a suitable replacement can be found.

c. Personnel nominated for a JPAS account must meet the following requirements per reference (y):

(1) Completion of a current Access National Agency Check with Written Inquiries for a final Secret security eligibility and access.

(2) Completion of a Single Scope Background Investigation or Periodic Reinvestigation for a Top Secret and SCI eligibility and access.

d. Prior to approval, each individual must accomplish the following tasks:

(1) Fill out a Personnel Security System Access Request (PSSAR) form and forward it to the Security Division via FAX (b)(7)(E) @ncis.navy.mil). This form must be signed by either your supervisor or security coordinator.

(2) Submit a letter of appointment (LOA) to the Security Division. Military account applicants are not required to submit an LOA. The LOA must be signed by the SAC or DAD and include applicant's name, SSN, contact information (office location, telephone number, e-mail address) and justification of specific job duties that require JPAS access. LOAs must remain on file for the lifetime of the account, plus six months after termination of account by the Security Division.

(3) Complete Mandatory Training. Prior to account approval, applicants must complete Cyber Awareness and Personally Identifiable Information (PII) training. These training courses may have been completed by applicants during annual refresher training. If not, the following training is available:

(a) Cyber Awareness Challenge/Security Training:

(b)(7)(E)

(b) Personally Identifiable Information (two options):

1. (b)(7)(E)
2.

(4) When the account has been created, you will receive an e-mail notification from the Security Division. Use your CAC when logging in. Username and password are no longer required to access JPAS.

e. When attempting to access the system, users may find their accounts locked due to inactivity or failure to log-off properly. When this occurs, send an e-mail to the Security Division at securityoffice@ncis.navy.mil, requesting assistance. A representative from the Security Division will perform the requested action and send a return e-mail to the individual, when the action is completed.

(1) In cases where a lock-out occurs due to failure to log-off properly, wait 30 minutes and try logging on again. If you still are unable to log in, contact the Security Division for assistance.

(2) JPAS accounts are automatically locked after 60 days of inactivity. When this occurs, the account will remain locked until the Security Division receives verification that the user still requires a JPAS account.

(3) JPAS accounts are automatically deleted by the system when inactive for over 90 days. When this occurs, the account holder must request a new account by following the guidelines in paragraph 36-26d above.

Appendix A: Definitions

1. Administrative Sanction. Non-judicial or disciplinary action which may be taken against any military, civilian, or support contractor employee who violates the provisions of applicable DoD Directive.

2. Classified National Security Information (or Classified Information). Information that has been determined pursuant to Executive Order 13526, reference (z) or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

3. Compromise. An unauthorized disclosure of classified information.

4. Controlled Unclassified Information. Unclassified information to which access or distribution limitations have been applied per national laws, policies, and regulations of the originating country.

5. Emergency Action Plan (EAP). A set of procedures outlining the steps to be taken during specific emergencies.

6. Foreign National. A person who is not a citizen or national of the United States.

7. Foreign Visit System. The automated system, operated by the Office of the Under Secretary of Defense (Policy) ((OUSD(P)), that provides staffing and database support for processing requests for visits by foreign nationals to DoD activities and defense contractors. FVS consists of an unclassified segment that allows the on-line submission of visit requests from embassies in Washington, D.C. and, in some cases, directly from foreign governments overseas. The FVS also has a classified segment that provides staffing, decision-making support, and database capabilities to the Military Departments and the Defense Intelligence Agency.

8. Inadvertent Disclosure. A security incident in which a person has involuntary, unauthorized access to classified information.

9. Incident. An act or circumstances in which there is a deviation from the requirement of the governing security regulations. Compromise, inadvertent disclosure, need-to-know violation (when involving classified national security information), and administrative deviation are examples of security incidents.

10. Indoctrinated Person. An individual granted access to SCI, who has been provided a briefing which includes the unique nature of SCI, its unusual sensitivity, and the special security regulations and practices for its handling.

11. Information Assurance Manager (IAM). The individual assigned responsibility for managing the information systems security posture of a Department of Defense Intelligence Information System (DoDIIS) site.

Appendix A (Continued)
Definitions

12. Information Assurance Officer (IAO). The individual responsible to the Information Assurance Manager for ensuring the appropriate operational information assurance posture is maintained for a field office, NCIS resident agency (NCISRA), NCIS resident unit (NCISRU), system, or enclave.

13. Inquiry. An examination into a reported security incident. This includes checking records, reviewing applicable directives, and interviewing persons with direct knowledge of a particular matter.

14. Inquiry Officer. Anyone detailed by an appointing authority (Chief, Security Division) to conduct an inquiry. An inquiry officer should be anyone competent, mature, and senior to the person who may have caused the incident.

15. Open Storage. The storage of classified material on shelves, in unlocked file containers, or unlocked GSA-approved security containers, within facilities where classified information is processed, while such facilities are not occupied by authorized personnel.

16. Security Assurance. A written confirmation by a responsible foreign government official that the proposed visitor possesses the requisite security clearance and need-to-know for the classified information and controlled unclassified information to be released during the visit. The security assurance certifies that the recipient government will protect the information per the international agreement between the United States and the foreign government.

17. Senior Intelligence Officer (SIO). The highest-ranking individual who is charged with direct foreign intelligence missions, functions, and responsibilities within a command or an intelligence community. Within NCIS, the Director is the SIO.

18. Sensitive Compartmented Information (SCI). Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled exclusively within formal access control systems established by the Director of National Intelligence (DNI).

19. Sensitive Compartmented Information Facility (SCIF). An accredited area, room, group of rooms, or installation where SCI may be stored, used, discussed or electrically processed. SCIF procedural and physical measures prevent the free access of persons unless they have been formally indoctrinated for the particular SCI authorized for use or storage within the SCIF.

20. Special Security Officer (SSO) System. The system through which the Director, DIA and NCIS perform their responsibilities for the security, use, and dissemination of SCI to include both physical and electrical means.

Appendix A (Continued)
Definitions

21. Special Security Officer (SSO). The individual with SCI security cognizance for the parent units supported and all subordinate SCIFs. The SSO is directly responsible to the Security Manager and SIO.

22. Special Security Representative (SSR). The individual (and alternate) responsible for the day-to-day management and implementation of SCI security and administrative management for a separate subordinate SCIF.

Appendix B: Newcomer Indoctrination/Orientation Guide

1. Security coordinators must conduct an orientation briefing for all newly assigned personnel. This briefing must be signed and forwarded to the Security Division for inclusion in the employee's security file.

2. The following are topics that should be discussed in person by the security coordinator with all newly assigned personnel, regardless of the individual's security clearance and/or access level or amount of previous classified information handling experience:

_____ Security requirements related to specific duties and/or particular assignments

_____ Accounting procedures for classified information

- Logging procedures

_____ Storage requirements

- Where/how classified information is stored

- Security Container Check Sheet (SF 702), its purpose and use

_____ Reproduction

- When to obtain approval

_____ Transmission

- Electronic transmission of classified information

- Hand-carrying within NCIS facilities

- Hand-carrying off military installations

- Hand-carrying aboard commercial aircraft

- Mailing procedures

_____ Destruction

- Approved methods

_____ Discussion of classified information

- Prohibited over non-secure telephone

Appendix B (Continued)
Newcomer Indoctrination/Orientation Guide

- Using STE/STU-III terminals

- Within close proximity of other personnel

_____ End-of-day security checks

- Procedures

- Responsibilities

- Checklists

_____ Access to classified information

- Determining “need to know”

- Providing access to NCIS personnel

- Providing access to visitors

_____ Security Incidents

- Reporting procedures

- Inquiries

_____ _____
Employee Name (printed) Date

_____
Employee Signature

_____
Security Coordinator Signature

Appendix C: Newcomer On-The-Job Security Briefing Guide

1. Supervisors will ensure that, as a minimum, the following information is conveyed to newly assigned personnel, regardless of length of service, rank or grade. The results of this briefing must be documented in the individual's locally held personnel file and include the date of the briefing and the name of the personnel responsible for presenting the briefing.

2. The following topics should be discussed in person with the newly assigned military personnel or civilian employees, regardless of the individual's security clearance and/or access level or amount of previous classified information handling experience:

__ Security requirements related to specific duties and/or particular assignments. This should include the level and type of classified information with which the individual will be working.

__ Receiving classified information. Outline mail receipt, hand carrying, and transferring of classified information.

__ Accounting. Discuss the types and levels of classified information that require logging and those that do not. Specifically address procedures related to how the information/material is logged, routed, and continuously accounted for.

__ Storage. Identify where and how classified information is stored.

__ Reproduction. Outline under what circumstances approval is first required prior to reproducing classified information. Identify when and how reproduced copies are handled.

__ Hand-carry. Address exactly how and under what circumstances, classified information may be hand-carried within NCIS office spaces. Also, establish protocols for transporting classified material outside of NCIS office space protocol on the same installation, off the installation, and via commercial aircraft. Include information regarding use of cover sheets, double wrapping, courier cards, and letters of authorization for hand-carrying on commercial aircraft.

__ Transmission. Discuss mailing procedures, message handling and use of STE/STU-III and secure fax. Specifically address prohibition of transmitting classified information via unsecured fax and unclassified e-mail.

__ Destruction. Identify approved methods of destruction for classified information and approved destruction devices, such as shredders or at a local DoD Classified Waste Facility. Address accounting and control procedures and need to document destruction for accountable classified.

__ Discussion. Advise that discussion of classified information over non-secure telephone, or within close proximity of personnel with no security clearance and/or need-to-know, is prohibited. Address authorized use of STE/STU-III terminals for classified discussion and use, control, and safeguarding of the terminal and card/key.

Appendix (C) (Continued)
Newcomer On-The-Job Security Briefing Guide

__ End-of-day security checks. Provide incoming personnel with a typical end-of-day security check. Identify how responsibilities are assigned. Demonstrate use of Standard Forms (SF) 702, Security Container Check Sheet, and SF 701, Activity Security Checklist. When applicable, thoroughly train the individual on how to activate/deactivate the alarm system.

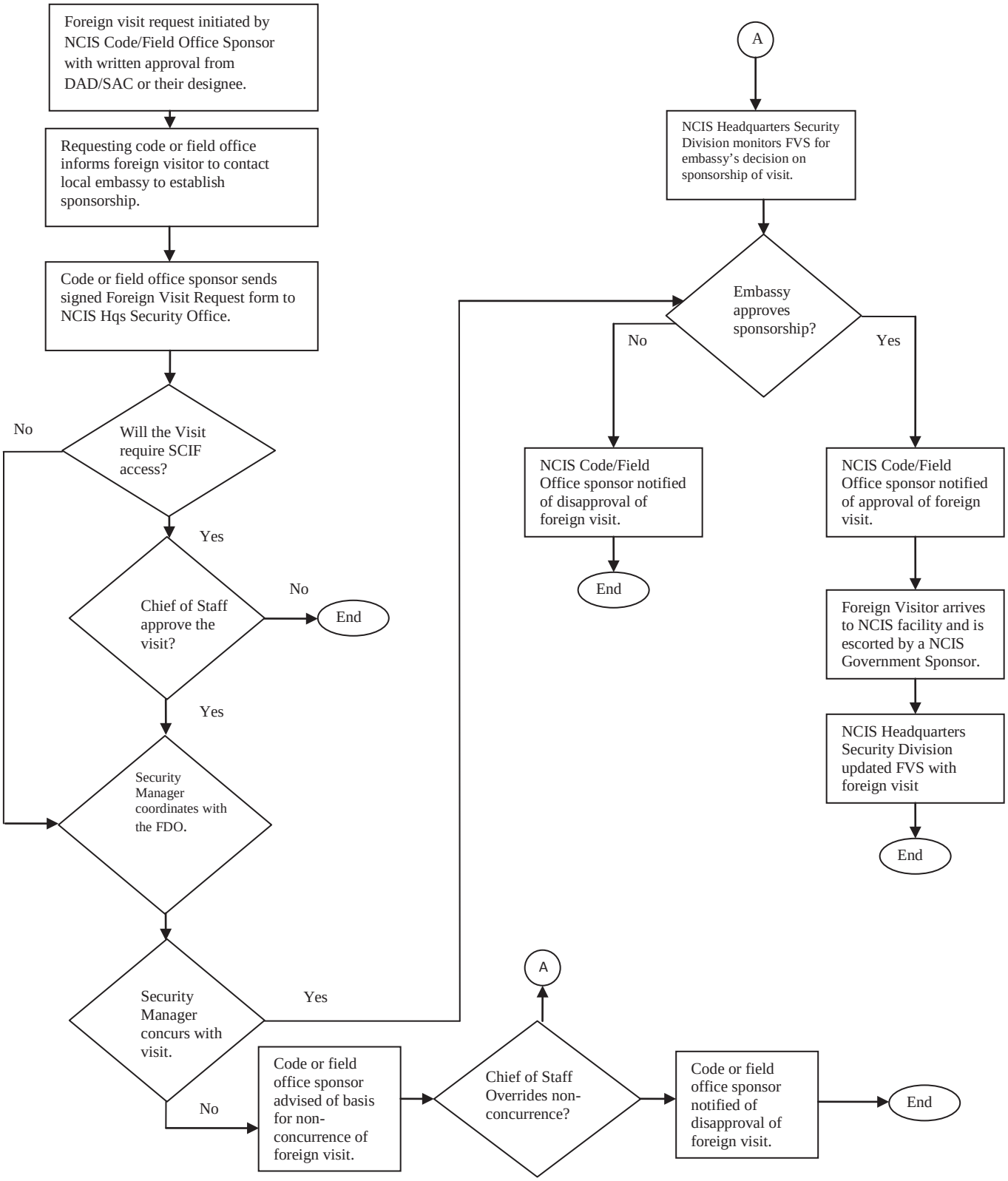
__ Visitor control. Address how visitors are admitted and controlled within NCIS office spaces, to include escorting requirements, classified and unclassified visits, where access approval has been arranged prior to such visits. Also address how to handle unscheduled visits.

__ Access to classified information. Reinforce that the individual possessing classified information is responsible for determining whether another properly cleared individual possesses the need-to-know. Address how to make such a determination and when it would be appropriate and/or inappropriate to provide such access.

__ Badge use. Where badges are used for access control, discuss different types of badges and their purpose, how they are displayed, and how to challenge individuals, not personally known, but observed without properly displaying an access badge.

__ Automated Information Systems (AIS) use. Review use of AIS equipment when processing classified information. Discuss logging on and off, prohibition of interchanging CD's and diskettes between unclassified and classified systems, periodic password changes, classification and marking of AIS generated hard copy, prohibitions and limitations of e-mail and other communication systems relating to classifications levels, etc.

Appendix D: Flowchart For CONUS Foreign Visit Request



Appendix E:
Sensitive Compartmented Information Security Standard Operating Procedures

1. Policy

a. This SOP establishes SCI security management policies and procedures for NCIS SCIFs. It applies to SCI indoctrinated personnel assigned to or employed by the NCIS. Each individual assigned or with access to a SCIF must read this SOP and certify in writing, by completion of Appendix (F), indicating they understand and will comply with the established security processes, actions, and procedures. Appendix (F) will be maintained in the employee's personnel security file for Headquarters personnel and in the local personnel file for field elements.

b. This SOP provides security requirements for NCIS SCIFs where SCI may be stored, used, discussed and/or processed. Each SCIF will develop an annex to this SOP to define local policies and procedures. All annexes to this SOP will be approved by the NCIS Special Security Officer (SSO) and maintained on file at both the NCIS SSO Office and in the affected SCIF. Appendix (G) provides a standardized template that can be used to create an annex.

2. Responsibilities

a. Special Security Officer (SSO). The SSO is responsible to the Chief, Security Division for the daily operations of SCI policy, processes, and programs within the NCIS enterprise. The SSO manages all SCI information, personnel, and physical security functions for NCIS Headquarters and field offices worldwide.

b. Special Security Representative (SSR). The SSR is a properly cleared and indoctrinated GS-7 or above, that has been assigned additional duties to manage the SCI security program of the respective field office. The SSR is responsible to the DAD, SAC and NCIS SSO for all SCI security matters within their geographic area of responsibility.

c. DADs and SACs. DADs and SACs for HQ codes or field offices that have a sensitive compartmented information facility (SCIF) are responsible for providing supervision and oversight to the SSR on SCI matters within their geographic area of responsibility.

3. Physical Security

a. The NCIS SCI Physical Security Program involves the accreditation of all NCIS SCIFs worldwide. The NCIS SSO spearheads all facets of SCIF physical security including coordination with SSO Navy and DIA for concept approval and accreditation/de-accreditation.

b. The SSR will serve as the primary focal point between the headquarters code or field office and the NCIS SSO for all physical security matters pertaining to their SCIF. Duties include maintaining the local SCIF file, ensuring proper operation of alarms and physical security devices, and maintaining access control for the facility. The SSR is responsible for ensuring that the periodic physical security requirements of reference (dd) are completed. These requirements include the annual SCIF self-inspection and semi-annual alarm testing. SSRs will

Appendix (E) (Continued)
Sensitive Compartmented Information Security Standard Operating Procedures

complete annual SCIF self-inspections and submit results to the NCIS SSO by 1 October of each year. The SSR will also document each requirement in the local SCIF file and report the results to the NCIS SSO. The SSR will contact the NCIS SSO regarding all physical security issues for the SCIF. If an emergency occurs after duty hours, ensure the NCIS SSO is contacted the next duty day and advised of actions taken to correct a security problem.

c. The following procedures apply to all NCIS SCIFs:

(1) SCIF Occupation. When open, the SCIF must be continually occupied by at least one SCI indoctrinated staff member. If only one person is occupying the SCIF and needs to leave the facility (e.g., restroom, get a drink, etc.), they may do so for one hour or less. During this short absence, the SCIF door must be secured, but it *does not* need to be alarmed. For absences longer than one hour, the SCIF must be secured and alarmed.

(2) SCIF Intrusion Detection System (IDS) Responsibilities

(a) The SSR will maintain a log documenting events regarding the IDS/alarm system. Mandatory entries include all maintenance, alarm indications, false alarms, alarm response results, and semi-annual testing.

(b) IDS Notification after Duty Hours. The monitoring station will be provided a list of NCIS personnel available to respond to alarm annunciations occurring after duty hours. Personnel will be prioritized on the list in terms of who is contacted first, second, etc. Personnel are responsible to respond to alarms within their respective facility.

(c) On receiving an IDS notification the monitoring station will contact the first person on the response list. If that person cannot be contacted, the monitoring team will continue down the list until a positive response to the alarm is made.

(d) The responding staff member must report immediately to the SCIF and meet the response force outside of the SCIF.

(e) The SCIF must then be accessed and inspected (both inside and outside the SCIF perimeter) for forced entry. (The response force will accompany the staff member during the SCIF walk-through.)

(f) If there is no evidence of forced entry, reset the alarm. The response may be terminated upon successfully resetting and activating the alarm system.

(g) The responding staff member will provide the SSO/SSR with a brief, written summary of the alarm response the next duty day.

Appendix (E) (Continued)
Sensitive Compartmented Information Security Standard Operating Procedures

(3) Catastrophic Alarm Failure. If the SCIF experiences a catastrophic failure of the alarm system, the facility must be manned by at least one SCI indoctrinated employee until the system becomes operational. The notification procedures outlined in paragraph 4c(2)(b) apply if the failure occurs after duty hours. Follow the procedures outlined in the EAP under "Loss of Essential Utilities." The NCIS SSO must be contacted if catastrophic alarm failure occurs.

d. Access Control. Only properly cleared staff personnel assigned to the SCIFs may possess the combination to the (b)(7)(E) Visitors must remain at the SCIF entrance area until their clearances have been verified. The SSO is the only official channel and point of contact (POC) for passing/receiving SCI access certifications. The following access control procedures will be followed:

(1) SCI Indoctrinated Visitors

(a) Visitors are responsible for forwarding their accesses prior to their visit. Visitor clearances will be maintained by the SSR or in JPAS. Contact the SSR or NCIS SSO for questions regarding clearance certification.

(b) Once the SSR/SSO has verified a visitor's SCI clearance, they can be granted access to the SCIF. The host official is responsible for meeting the visitor at the SCIF entrance and providing an escort.

(c) The host official will query all visitors regarding possession of prohibited items (listed in paragraph 4g(3) of this SOP) and ensure those items are controlled at the SCIF entrance.

(d) All non-NCIS personnel are required to sign the visitor log.

(e) Upon admittance to the SCIF, the visitor's host should advise resident staff members of the visitor's arrival and their clearance status.

(f) Upon conclusion of the visit, the visitor's departure time will be annotated in the visitor log.

(2) Non-indoctrinated Visitors. Access to the SCIF by non-SCI indoctrinated personnel is discouraged. When it is necessary to grant access to non-indoctrinated personnel, the following approvals are required.

(a) The SSR will approve non-indoctrinated visitors for building and equipment maintenance.

(b) The SSO will approve non-indoctrinated visitors for special circumstances.

Appendix (E) (Continued)
Sensitive Compartmented Information Security Standard Operating Procedures

(c) The SIO will approve non-indoctrinated visitors for open house events, promotion ceremonies, family orientation, etc.

(d) Once the visit is properly approved, the following procedures apply:

1. The host POC must announce the pending admittance of non-indoctrinated personnel to all staff members and ensure the SCIF is properly sanitized.

2. All visitors permitted entry to the SCIF will sign the visitor log.

3. The host POC will activate a warning beacon light or other suitable warning device (to remind resident staff members of the presence of non-indoctrinated visitors within the SCIF); this light must remain on for the duration of the visit.

4. The host POC will query the visitor regarding prohibited items and ensure those items are controlled at the SCIF entrance.

5. All non-indoctrinated visitors will be under constant visual escort while inside the SCIF.

6. SCI operations (including discussions) will cease whenever an uncleared visitor is in the immediate vicinity.

7. Personnel assigned to the SCIF will be SCI indoctrinated. Escorting non-SCI indoctrinated personnel to perform full-time duties is not authorized.

8. Upon conclusion of the visit, the visitor's departure time will be annotated in the visitor log.

(3) Foreign Visitors. Foreign visits will be approved per paragraph 36-25.

e. Combinations/Locks. The SCIF entrance doors and security containers have (b)(7)(E) (b)(7)(E) Records of each combination must be recorded on a Security Container Form, SF 700. The completed SF 700 will be maintained within a SCIF approved at the same or higher classification level. The SSO/SSR for each SCIF is responsible for changing combinations as needed.

f. Telephones. NCIS SCIFs are equipped with secure telephones for use in classified/unclassified conversation. Since these telephones are routinely used in close proximity between staff members, extreme care must be taken to ensure proper security is observed and maintained. Do not engage in classified conversation on a secure telephone while another staff member is close by and using an unclassified telephone system. Also remember:

Appendix (E) (Continued)
Sensitive Compartmented Information Security Standard Operating Procedures

(1) Never "talk-around" classified information when using a telephone that is not in the secure mode.

(2) If you must discuss classified information, go "secure."

g. Classified Waste. Each workstation shall have an unclassified trashcan and a classified waste burn bag. All food products, paper and non-paper (unclassified) waste shall be put in the unclassified trashcan. All classified paper waste will be destroyed using an NSA approved crosscut shredder or placed in a burn bag for later destruction. Burn bags must be marked with the highest level of classified material in the burn bag, and the individual's name, office, and phone number.

h. Control of Items Entering and Leaving the SCIF

(1) Incoming. All incoming equipment, furniture, supplies, and related items must be inspected to prevent the introduction of prohibited items, hazardous materials, and other items not authorized for use in the SCIF. Staff members bringing items into the SCIF or accepting delivery of such items will contact the SSO/SSR for assistance with the inspection.

(2) Outgoing. All outgoing equipment, furniture, waste material, and related items must be inspected prior to removal to ensure SCI or other classified materials are NOT contained in the objects being removed. Exception: burn bags containing classified material that are being transported for destruction. Personnel removing items from the SCIF will notify the SSO/SSR.

(3) Personal Electronic Devices (PEDs). NCIS Policy regarding the introduction of PEDs to spaces that process classified material is provided in paragraph 36-13 of this chapter. All NCIS SCIFs will strictly adhere to that policy. SSRs will maintain a readily available copy of this policy, and will refer any issues regarding this policy to NCIS SSO.

(a) Use of personally owned radios and CD players are permitted within each SCIF provided they do not have a recording capability. Personal CDs must NOT be played on government computer equipment.

(b) Visitors with any type of transmitting device (two-way radios, pagers with transmit capability, cellular phones, etc.) must leave these items at the SCIF entrance for safekeeping until departure. (Exception: emergency teams [police, fire, medical, etc.] responding to an emergency within the SCIF.)

(c) All electronic equipment introduced into the SCIF is subject to technical and/or physical inspection at any time. Contact the SSO/SSR prior to introducing electronic equipment into the SCIF.

Appendix (E) (Continued)
Sensitive Compartmented Information Security Standard Operating Procedures

(4) Entry and Exit Inspections. Entry and exit inspections of hand carried items (briefcases, etc.) may be conducted by the SSO/SSR or other staff members approved by the security office to:

(a) Ensure prohibited items, hazardous materials, and contraband are not introduced into the SCIF.

(b) Prevent unauthorized removal of classified material from the SCIF.

(5) After-duty-hours Inspections. The SSO may authorize random after-duty-hours inspections to occur at any time within the SCIF. The search can be limited in scope or include the whole facility. All random inspections will be coordinated with the information assurance manager. The inspection will be conducted by cleared and indoctrinated NCIS personnel.

i. "Open House" Type Activities. When "open house" or similar group activities involving admittance of non-cleared visitors are desired, the NCIS SIO must first approve such activity. Regular SCIF sanitization and access control procedures apply.

4. Personnel Security

a. Security Clearance Investigation. The NCIS Security Manager is responsible for security clearance investigations for NCIS personnel. This includes initiation of investigations, aiding NCIS personnel in completing needed forms, checking the forms for accuracy and completeness, and coordinating with the servicing personnel security office.

b. SCI Indoctrination. NCIS staff members who require SCI access must be prescreened and adjudicated for access prior to indoctrination. Supervisors must provide the SSO with a written justification for each employee requiring SCI access. The SSO will coordinate all SCI indoctrinations.

c. SCI Debriefing. NCIS staff members no longer requiring SCI access (e.g., permanent change of station, retirement, departure or resignation from civil/military service) shall be debriefed by the SSO. Contact the SSO to schedule a debriefing appointment.

d. Reporting Requirements

(1) Change of Personal Status. As an SCI indoctrinated individual, it is your responsibility to report changes in personal status to your supervisor and the SSO/SSR. Changes could include (but are not limited to): change of assignment, change of marital status, cohabitation, adverse involvement with law enforcement agencies, bankruptcy filing, credit judgments, foreclosure, short-sale, etc. Contact the SSO/SSR for further guidance.

Appendix (E) (Continued)
Sensitive Compartmented Information Security Standard Operating Procedures

(2) Foreign Contacts. NCIS staff members have the continuing responsibility to report foreign contacts of a "close and continuing nature characterized by ties of obligation or affection" to their immediate supervisor and the SSO/SSR within 72 hours. Casual contact and association arising from living in the community normally need not be reported. The SSO/SSR will review the circumstances regarding the contact and provide guidance based on the situation. Operational contacts documented in official reporting need not be reported to the SSO/SSR. When in doubt, report the foreign contact to the supervisor and SSO/SSR.

(3) NCIS staff members who have immediate family members or other persons who are non-U.S. citizens to whom the NCIS staff member is bound by affection or obligation may be eligible for access to SCI as a result of an "exception." Appendix (H) provides the NCIS policy in regards to submission of exception packages.

(4) Foreign Travel/Travel Restrictions. Personnel planning unofficial foreign travel must report anticipated travel plans to their immediate supervisor and the SSO/SSR. The SSO/SSR will provide information regarding threat conditions and provide a foreign travel briefing. Upon completion of the travel, each traveler must submit a foreign travel questionnaire to the SSO.

e. Passing/Receiving Clearances. The SSO is the sole authority for passing and receiving SCI clearances. The NCIS Security Manager manages administration and passing of NCIS personnel collateral clearances. Notify the Security Division of the need for passing your clearance five days in advance by completing an NCIS Form 5521/1. Contact the SSO/SSR when checking on the receipt of a visitors' clearance.

5. Information Security

a. Security Violations, Compromises, or Possible Compromises. All security violations, compromises, or possible compromises must be reported to the supervisor, the SSR, and the SSO ***IMMEDIATELY***. An NCIS supervisor, designated by the Security Division, will conduct a preliminary inquiry and provide the NCIS SSO and Security Manager with the results of the inquiry.

b. Courier Authorization. A courier card is required if you must transport SCI material from one SCIF to another. Contact the SSO/SSR for a courier card and authorization to courier SCI materials locally. If you must courier SCI material outside the local area and/or aboard aircraft, contact the NCIS SSO. The SSO will review requests, provide courier instructions and training, and coordinate approval.

c. Defense Courier Division. SCI information cannot be sent via the U.S. Postal System or any commercial cargo/shipping company. The Defense Courier Division (USTRANSCOM) is the only authorized method for shipping SCI material. The SSO/SSR will serve as the primary POC for all Defense Courier Division transactions/accounts.

Appendix (E) (Continued)
Sensitive Compartmented Information Security Standard Operating Procedures

d. Security Education Awareness/Training. The NCIS SSO has a continuing SCI security education, awareness, and training program. This program is incorporated into the Security Division's annual TWMS security awareness training and education. Contact the SSO/SSR for questions regarding the security education and training program.

e. Classification and Marking. All SCI documents will be properly marked with classification and handling caveats. Refer to the appropriate program security classification guide for specific marking requirements. Questions regarding classification markings should be directed to the SSO/SSR.

f. Reproduction of Classified Materials. Reproduction of classified material is only permitted on copiers marked for classified reproduction. Copy only the minimum amount necessary. Do not use facsimile machines for reproduction of classified material.

g. Copier Maintenance. If maintenance personnel must service a copier, the escorting official must always run five blank copies through the machine prior to servicing. Personnel must be under constant visual escort while providing maintenance to copiers in the SCIF.

h. Document Destruction. Documents should only be retained for as long as they are needed. When a document is superseded or outdated, destroy the document by using the crosscut shredders located within the SCIF.

i. Release of Information

(1) Public Release of Information. NCIS personnel will ensure that information generated or received under their control is not made available for use in public speeches or testimony. Requests for information shall be referred to the Communication Directorate (Code 00C) or the NCIS Freedom of Information Act (FOIA) Office as appropriate.

(2) Pre-Publication Review Responsibility. SCI indoctrinated or debriefed personnel must submit to the NCIS SSO for security review (prior to public disclosure in any form):

(a) All material intended for disclosure that may contain SCI or SCI-derived information.

(b) All proposed public statements on information derived from SCI or concerning SCI operations, sources, or methods.

(c) Resumes or applications for employment that detail technical expertise gained through government employment in classified or sensitive programs that might contain SCI.

6. Communications, Information Systems (IS), TEMPEST Security. Electronic processing equipment within NCIS SCIFs requires two accreditation approvals - a TEMPEST accreditation

Appendix (E) (Continued)
Sensitive Compartmented Information Security Standard Operating Procedures

or Inspectable Space Determination (ISD) and an automated information system (AIS) accreditation. Electronic processing is not authorized until both accreditation approvals are received.

a. Communications/TEMPEST

(1) An ISD was performed by the Defense Intelligence Agency (DIA) on NCIS SCIFs; it defines the TEMPEST countermeasures applicable to NCIS SCIFs.

(2) The NCIS SCIFs are TEMPEST approved for electronic processing equipment. NCIS personnel must contact the NCIS IAM when introducing, moving, or replacing electronic processing equipment in each of these areas. The NCIS IAM will evaluate the equipment's TEMPEST vulnerabilities and provide the user with required TEMPEST countermeasures as assigned by DIA.

b. Minimum Security Requirements for Users of Information Systems (IS)

(1) The computer security guidance, reference (aa), applies to all NCIS personnel using NCIS IS. This includes information systems operating in all NCIS SCIF and NCIS laptops and computers issued to personnel.

(2) Personnel with access to NCIS IS must be cleared to the highest level of information ever processed on the information system and shall be approved for access by submitting a Remedy ticket approved by their supervisor. Personnel will not be issued an account until verification that IA training has been completed and a System Authorization Access Request (SAAR) form is on file with the IAM. Visitors to the SCIF are not authorized to access NCIS information system without permission from the IAM.

(3) NCIS ISs are considered DoD national security interest computer systems. DoD computer systems are provided for the processing of official U.S. Government information only. Use of DoD computer systems is restricted to authorized users. DoD computer systems will be monitored to ensure information security system integrity and the limitation of use to official purposes. The use of DoD computer systems constitutes consent to monitoring as an integral part of system management. Information derived from system monitoring may be used as a basis for administrative, disciplinary or criminal proceedings. Your use of an NCIS information system provides your total and unequivocal understanding of the agreement which will be displayed on the IS to which you must agree before logging into information system. **Your use of an NCIS IS is subject to monitoring.**

(4) Users shall use the information system for official and appropriate use only. Personal use of IS is prohibited.

(5) Users will have a required unique USERID and password or Common Access Card

(CAC) in order to access information systems. All USERID and passwords must be protected at the same security classification as the system. Users will not share their password with others. Password must be changed if it has been compromised or has expired.

(6) Users will read the system logon-warning banner and acknowledge its content prior to being granted access to the information system.

(7) Users are required to logout of systems at the end of each workday or for an extended absence.

(8) Hardware or software will not be installed and/or connected to any computer system/network without approval from IAM and performed by IT personnel.

(9) All hardware and software connections, modifications, and installations must be approved by the IAM and installed by IT personnel.

(10) Only authorized software is permitted on information systems and shall be approved by the IAM. Unauthorized software includes, but is not limited to, games, shareware, personally owned software, or software from unknown sources.

(11) Ensure virus scanning application is loaded on system and functioning. Ensure that all media introduced to the information system are scanned for malicious code.

(12) Thumb drives are not authorized in SCIFs. They are not to be used in SCI systems.

(13) Removable information storage media (e.g., CDs, disc packs, cassettes, cartridges) will be labeled indicating the classification of the information. For CDs containing classified data, label the CD storage case in addition to the CD itself.

(14) Hardware (e.g., CPUs) should be labeled with the classification of information processed on the system and use of the SF 700 series is recommended.

(15) Transferring of information from information systems of different classification (e.g., SIPR and JWICS) must be performed through the Cross Domain System.

(16) Users are to report all security incidents and/or potential threats and vulnerabilities on information system to the IAM or IAO immediately.

c. Computer Start-up Procedures. Before using the system:

(1) Verify information systems approved to process the highest level of information to be used during processing session.

Appendix (E) (Continued)
Sensitive Compartmented Information Security Standard Operating Procedures

(2) Briefly inspect the equipment for signs of tampering (screws missing, pry marks, scratches). If you find such signs, immediately notify the IAM or IAO.

(3) When powering the IS up, verify engagement of the anti-virus software for checking the system for viruses.

(4) When powered up, ensure there is a classification banner on top of information system to indicate the system security level.

(5) When logging in, ensure the DoD warning banner is displayed.

d. Maintenance. Only authorized personnel are permitted to perform maintenance on IS. The NCIS IT department is responsible for all IS in the SCIF. Contact the NCIS IT department for assistance. NOTE: Users are NOT allowed to perform maintenance or make modifications or tamper with any equipment. The IT staff will accomplished the following steps prior to access by contractor personnel:

(1) Remove all classified data from the system, including on or around the printer.

(2) If possible, recall several unclassified files into system memory or clean memory.

(3) DO NOT provide classified diskettes, hard drives, or ribbons to maintenance personnel for system testing. Use unclassified media only.

(4) An authorized system operator must stand by and observe all maintenance activities. Report any suspicious practices to the SSO/SSR.

e. Backup Procedures. The NCIS IT department does not backup local hard drives. If you place data on your local machine and do not regularly save it to the network, you are responsible for ensuring your local data is backed up to CDs and appropriately marked with the proper classification.

f. Relocation of Computer Equipment. Information system equipment must NOT be removed from the SCIF or moved to different locations within the SCIF without prior approval of the IAM. Moving computer equipment without approval could violate the system SCI accreditation and create the problem of non-compliance. Certain distance requirements between computer equipment and other electronic equipment (e.g., telephones, other computer systems, networks, etc.) are practiced for reasons of operating security. Contact the NCIS IT department prior to movement of computer systems and equipment.

g. Sanitization. All classified media remain classified and controlled until explicitly declassified. It is NCIS policy to destroy SCI magnetic media once it is no longer needed. Users should contact NCIS IT department, IAM or IAO to provide any media for destruction.

Appendix (F): SCI SOP Acknowledgement of Understanding

Sensitive Compartmented Information
Acknowledgement of Understanding

Date: _____

I _____ certify that I have read and understand the contents
Print Name
of the Sensitive Compartmented Information (SCI) Standard Operating Procedure (SOP). All of my questions have been answered by the Special Security Representative or Special Security Officer. I will comply with the contents of this SOP and any local annex's presented.

_____
Signature

Appendix (G): Site Specific Annex

Field Office Letterhead

Date

Site Specific Annex: Sensitive Compartmented Information (SCI) Security Standard Operating Procedure (SOP)

Note any operating procedures not previously referenced, not applicable or different than the original Appendix F SCIF SOP.

NOTE: Every site has unique circumstances. The purpose of this annex is to document these circumstances. Please contact the NCIS SSO for additional guidance, if required.

1. Physical Security: *Please reference anything site specific regarding Physical Security. Examples would be: Phone numbers for alarm POC's, deviations from standard access control, 24/7 operations, etc.*

a. SCIF Opening and Closing Procedures

(1) Opening.

(2) Closing.

(3) SCIF Occupation.

b. SCIF Alarm System Responsibilities

(1) Alarm Activation After Duty Hours.

(2) Catastrophic Alarm Failure.

c. Access Control:

(1) SCI Indoctrinated Visitors

(2) Non-Indoctrinated Visitors.

(3) Foreign Visitors.

d. Combinations/Locks.

e. Telephones.

Appendix (G)
Site Specific Annex (Continued)

f. Classified Waste.

g. Control of Items Entering and Leaving the SCIF:

(1) Incoming.

(2) Outgoing.

(3) The following items are strictly prohibited in the SCIF.

(4) Entry and Exit Inspections.

(5) After-duty-hours Inspections.

h. "Open House" Type Activities.

2. Personnel Security. *Please reference anything site specific regarding Personnel Security. Examples would be: Reporting requirements, interim clearances, personnel folders.*

a. Security Clearance Investigation.

b. SCI Indoctrination.

c. SCI Debriefing.

d. Change of Personal Status.

e. Foreign Contacts.

f. Foreign Travel/Travel Restrictions.

g. Passing/Receiving Clearances.

3. Information Security. *Please reference anything site specific regarding Information Security. Examples would be: IT system protection, prohibited item waivers (cell phones, recording devices, etc.)*

a. Security Violations, Compromises, or Possible Compromises.

b. Courier Authorization.

c. Defense Courier Service.

Appendix (G)
Site Specific Annex (Continued)

d. Security Education Awareness/Training.

e. Classification and Marking.

f. Reproduction of Classified Materials.

g. Copier Maintenance.

h. Document Destruction.

i. Release of Information.

4. Communications, Information Systems (IS), TEMPEST Security. Electronic processing equipment within NCIS SCIFs requires two accreditation approvals - a TEMPEST accreditation or Inspectable Space Determination (ISD) and an automated information system (AIS) accreditation. Electronic processing is not authorized until both accreditation approvals are received. *Please reference anything site specific regarding IS, TEMPEST Security. Examples would be: TEMPEST waiver requests, processing deviations, etc.*

a. Communications/TEMPEST.

b. Minimum Security requirements for users of IS.

c. Computer Start up Procedures.

d. Maintenance.

e. Backup Procedures.

f. Relocation of Computer Equipment.

g. Sanitization.

Appendix (H)
Processing Exception Requests for Access to Sensitive Compartmented Information for Employees with Non-U.S. Citizen Immediate Family Members

1. The purpose of this policy document is to summarize existing policies, standards and processes for SCI access and provide implementing guidance for requesting exceptions to that policy.

2. References (bb) and (cc) establish the National Intelligence Community and DON eligibility standards for access to SCI, respectively. The foundation of these standards includes:

a. The subject requiring access to SCI must be a U.S. citizen.

b. The subject must be stable, trustworthy, reliable, discreet, of excellent character, must possess sound judgment, and must be unquestionably loyal to the United States.

c. Members of the subject's immediate family and any other person(s) to whom the subject is bound by affection or obligation shall not be subject to physical, mental, or other forms of duress by either a foreign power or by persons who may be or have been engaged in criminal activity, or who advocate either the use of force or violence to overthrow the U.S. Government, or alteration of the form of the U.S. Government by unconstitutional means.

3. Subjects who have immediate family members or other persons who are non-U.S. citizens to whom the subject is bound by affection or obligation may be eligible for access to SCI as a result of an "exception." This section provides NCIS policy with regard to submission of exception packages for its personnel.

4. Access to SCI is adjudicated using a risk management system to weigh the risks of permitting access for an individual who does not meet the eligibility standards against the need to maintain national security within the National Intelligence Community. Exceptions to the personnel security standards shall be based on a finding that the risk to national security is manageable and acceptable.

5. Within the NCIS enterprise, the SSO will be the single point of contact for NCIS hiring managers, human resource professionals, and leadership to assist in determining whether individuals will require SCI access, what risk assessment level is currently assigned to foreign countries, and will be the process owner for the exception process.

6. Reference (cc) provides a country matrix decision aid that assigns countries to a low, medium, or high tier based upon the foreign intelligence and terrorism threat posed by the country. This decision aid shall be used to determine the prescreening and continuous evaluation requirements for an individual with non-U.S. citizen immediate family members or others, based upon their country of citizenship. Granting SCI access eligibility to individuals with non-U.S. citizen family members will be based on assessment of country risk and the need for the individual's services.

Appendix (H) (Continued)
Processing Exception Requests for Access to Sensitive Compartmented Information for Employees with Non-U.S. Citizen Immediate Family Members

a. For countries that are designated as "LOW TIER", the risk has been determined to be negligible and as such, requires only favorable adjudication by the DoD CAF, Navy Division and SSO verification of the family member's citizenship.

b. For "MEDIUM TIER" and "HIGH TIER" countries:

(1) A compelling need must exist for the individual's services that justify mitigating risk to national security prior to SCI processing. To document this compelling need, supervisors will draft and submit a Compelling Needs Statement (CNS), based upon specific national security considerations, that describes the unique skills possessed by the individual and/or other special considerations or circumstances (e.g., the skill pool available is very limited; the mission to be performed is of extraordinary importance; and/or the individual's services are critical to mission accomplishment). Individuals who are currently indoctrinated for SCI access are not required to have a CNS. By virtue of working the mission with a presumed value of the individual's current participation in SCI programs, the compelling need is considered self-evident.

(2) An Intelligence Risk Assessment (IRA) will be prepared by the supervisor, specifically related to the individual's position. The IRA considers the country in question, its current threat assessment, and the employee's exposure to U.S. intelligence products relating to the foreign national's country of origin. For example: Does or will the individual's duties involve exposure to U.S. intelligence products relating to the country of origin of the foreign national who is the subject of the exception request? How might this factor influence the individual's assignment to such duties?

(3) The individual will provide an up-to-date copy of their SF-86, Personnel Security Questionnaire.

(4) The nominated individual will complete and submit a Foreign Born Spouse Statement of Personal History (FBS/SPH) and a copy of the prospective spouse's birth certificate, passport or other evidence of current citizenship, translated into English, to be included with the exception package.

(5) NCIS SSO will provide supervisors with formatting and content requirements for the CNS/IRA package.

c. Supervisors will submit the CNS/IRA package to SSO NCIS to submit for executive review. The complete "exception package" will be forwarded to the Director, NCIS for final signature. As the Senior Intelligence Officer, the Director NCIS is solely responsible for confirming the validity of an exception request. The review is documented by favorable endorsement of the CNS/IRA. If the Director does not concur with the validity of the CNS/IRA, the individual will not be nominated for access to SCI and the process is terminated without prejudice. Disapproval of the CNS/IRA package will be filed in the individual's SSO file.

Appendix (H) (Continued)
Processing Exception Requests for Access to Sensitive Compartmented Information for Employees with Non-U.S. Citizen Immediate Family Members

d. When the NCIS Director approves the CNS/IRA package, the NCIS SSO will request a "Signal Flags" check from SSO Navy, and in the cases involving HIGH-TIER countries, coordinate the completion of a CI interview conducted by NCIS Code 22B and submit the package to DONCAF.

NCIS-1, CHAPTER 37
EMERGENCY AND EXTRAORDINARY EXPENSE FUNDS
EFFECTIVE DATE: APRIL 2013

TABLE OF CONTENTS:

References:
(a) 10 U.S.C. § 127, Emergency and Extraordinary Expenses
(b) SECNAVINST 7042.12, Guidelines for the Use of Emergency and Extraordinary Expense Funding other than Official Representation Funds
(c) 5 U.S.C. § 5536, Extra Pay for Extra Services Prohibited
(d) SECNAVINST 5720.42F, Department of the Navy Freedom of Information Act Program
(e) 5 U.S.C. § 4501-4507, Awards for Superior Accomplishments
(f) Department of Defense (DoD) Financial Management Regulation (FMR) 7000.14-R
(g) NCIS Manual 3, Chapter 8, Central Source Registry
(h) 5 U.S.C. § 5702, Per Diem; Employees Traveling on Official Business
(i) NCIS Manual 3, Chapter 35, Protective Operations
(j) NCISINST 5000.64, Defense Property Accountability System (DPAS) Management and Administration
(k) NCIS Manual 1, Chapter 7, Supply, Property, and Equipment
(l) DoD Instruction S-5240.9, Support to Department of Defense Offensive Counterintelligence Operations (U)
(m) NCIS Manual 3, Chapter 9, Criminal Reduction Operations
(n) NCIS Manual 3, Chapter 13, Evidence Custody System
(o) DFAS-CL/FFA Memo dated 29 Jun 1995

37-1. Purpose

a. Reference (a) provides statutory authority to the Secretary of the Navy (SECNAV) for the expenditure of funds which cannot be anticipated or classified. Reference (b) delegates such authority to the Director of the Naval Criminal Investigative Service (DIRNCIS) for the purpose of gathering information on criminal or counterintelligence activity involving the Department of the Navy (DON) and persons of interest thereto, procuring evidence of such, and providing protective security services to such persons as deemed appropriate by the SECNAV.

b. The provisions of this chapter apply to civilian employees, active duty and reserve military personnel assigned to, or operating under the authority of, NCIS. The procedures established in this chapter are written to prevent waste, fraud, abuse, and mismanagement and are a part of the NCIS Manager's Internal Control Program. Violations of the policies and procedures set forth herein may result in administrative, disciplinary or judicial (criminal) proceedings.

37-2. Policy Statement. This chapter establishes policies and procedures for the expenditure and accounting of Emergency and Extraordinary Expenses (EEE) funds.

37-3. Cancellation. NCIS 1, Chapter 37 dated May 2008.

37-4. Chapter Sponsor. The sponsor for this chapter is the NCIS Comptroller, Financial Management and Planning Directorate (Code 00F), with assistance from the Office of the Inspector General (IG).

37-5. Authorized/Prohibited Uses. The use of EEE funds is limited to situations wherein security considerations, timeliness, opportunity, or other circumstances peculiar to the collection of investigative information, prevent the use of other Navy appropriations. Specific prohibitions include the following:

a. Reference (c) bans the use of EEE funds to supplement the pay, allowances, and entitlements of personnel employed in either a civilian or military capacity by the Department of Defense (DoD) for performance of functions within their established scope of duty.

b. EEE funds may not be used to facilitate activities precluded by statute or appropriate authority.

c. EEE funds may not be used to facilitate activities conducted by another agency of the United States Government unless conducted in concert with NCIS authorized operations.

d. EEE funds may not be used to purchase printed stationery, to include seasonal/greeting cards, thank-you cards, etc.

e. EEE funds may not be used to purchase gifts for U.S. Government employees.

f. EEE funds may not be used for the payment of membership fees to organizations (i.e., International Association of Chiefs of Police (IACP)) in the name of individuals, except where such membership is deemed essential by the special agent in charge (SAC) or NCIS headquarters (NCISHQ) deputy assistant director (DAD) in the pursuit of a specific operational mission. SAC or DAD approval is required.

g. Persons on temporary duty (TDY) may not claim expenses that are covered by per diem and miscellaneous entitlements.

h. Claims may not be approved by the same person who incurred an expense. For example, SACs and DADs must submit claims containing their expenses to their respective executive assistant director (EAD)/assistant director (AD) for approval.

i. Reference (a) requires any obligation or expenditure in excess of $500,000 to be separately reported to Congress. Accordingly, if any headquarters or field element anticipates a requirement which may require the obligation or expenditure of funds in excess of $500,000, the DIRNCIS, via the NCIS chain of command, must be immediately notified.

j. Authorized military and civilian personnel not attached to NCIS, but under NCIS supervision, may be provided EEE funds for specific and immediate use. As these personnel will usually not be aware of the contents of this chapter, including the prohibitions of use provisions, the supervising NCIS employee shall retain responsibility for proper safeguarding and utilization of EEE funds. Accordingly, liability for the funds shall remain with the NCIS employee. Sub-vouchers shall be prepared by the NCIS employee and will include the names of non-NCIS individuals involved in the expense.

37-6. Training. Personnel authorized to expend EEE funds are responsible for familiarizing themselves with and following the procedures established in this chapter. Special agents will be trained on EEE procedures during special agent basic training. Supervisory special agents (SSAs) will receive additional training during basic law enforcement supervisory training. Oversight officials (SACs, assistant special agents in charge (ASACs), senior intelligence officers (SIOs), field operations support officers (FOSOs), SSAs), fund custodians and paying agents will receive training on these procedures biennially.

37-7. Accountability

a. Proper use of and accountability for EEE funds is incumbent on all personnel authorized to expend and administer such funds. Due to the nature of their intended use, accountability must be maintained in a more stringent fashion than with other appropriations of the Federal Government. It becomes necessary, therefore, to avoid any and all expenditures that are, or may appear to be, improper. All personnel involved in the management, expenditure, authorization/approval and accountability of EEE funds must be aware that claims are routinely examined by internal and external audit entities, such as the NCIS IG, the Naval Audit Service and the DoD IG. Personnel expending EEE funds must always consider the value of the item or information being obtained, as well as the overall propriety and legality of the expenditure.

b. Expenditures of EEE funds will be reviewed by the appropriate chain of command to ensure compliance with this chapter using Appendix A through G. Deficiencies and discrepancies will be corrected or fully explained when identified. The submitter (claimant) of NCIS Form 029 signs the form to confirm that the expense occurred and that they have been fully reimbursed for any personal funds used. The claimant's supervisor signs the form to authorize reimbursement by the fund custodian. The fund custodian is responsible for aggregating the sub-vouchers onto NCIS Form 030 and ensures the claim is properly classified, the sub-vouchers are appropriately categorized and that the amounts on the form are accurate. Two optional levels of supervisory concurrence above the preparer may be used to indicate managerial review of the claims. The approver of the claim (normally SAC or DAD) is personally liable for the accuracy and propriety of the claim. The Comptroller will ensure all claims are reviewed by their office to ensure the claims for and uses of EEE funds are proper, in compliance with this chapter and documented for review by appropriate authority as required. Deficient claims will be referred to the submitting office/individual for correction or explanation. Such referrals will be tracked until resolved. Unresolved discrepancies will be referred to DIRNCIS for appropriate resolution.

37-8. Security Classification of EEE Documents

a. Documentation supporting the expenditure of EEE funds for law enforcement initiatives will be marked "For Official Use Only" (FOUO). Information designated FOUO must be protected from disclosure to those not authorized access to it. FOUO disclosure restrictions are outlined in reference (d). An e-mail originated by and sent to other NCIS personnel that use the NCIS Intranet may be utilized to transmit FOUO information.

b. Counterintelligence (CI) expenses will be classified as Confidential. EEE expenditures in support of the NCIS Fleet Operations Group (FOG) will be classified as Confidential. No EEE documents, including appended receipts and justifications for expenditures, shall exceed the Confidential security classification.

c. If, due to the security classification of an event or associated documentation, a full and complete justification for an expense cannot be provided, the claimant will reference corroborating documentation (i.e., in case files, report of investigation (ROI), intelligence information report (IIR), etc.) and the location of such documentation.

d. The undercover (UC) and true names of an NCIS undercover agent (UCA), cooperating witness (CW) or similar asset, should not be indicated on claims or appended receipts. When filing such claims, all reference to those names must be purged. If necessary due to the appearance of compromising information, receipts may be retained locally and the claim narrative annotated accordingly.

e. Established patterns of conduct or contact in sensitive operations and investigations will not be revealed. If a particular restaurant is used for operational contacts on a regular basis, then the name and location of that restaurant, as well as receipts, should not be included in claims. Again, local retention is authorized, with corresponding annotation to that effect in the claim narrative.

f. Information protected under special access programs will never be identified in any claim, sub-voucher, or associated documentation.

37-9. Categories of Expenditures

a. EEE expenditures will be listed as one of three types; law enforcement (LE), CI or FOG. Categories within these types are:

(1) Liaison.

(2) Bulk Mementos.

(3) Operational.

(4) Protective Operations.

(5) Non-Consumed Equipment.

(6) Undercover.

(7) Rewards.

(8) (b)(7)(E)

(9) Evidence.

(10) Miscellaneous.

b. No other categories of expenditures are authorized. Specific requirements for filing claims under these categories are described below:

37-9.1. Liaison. Liaison functions are held in an overt fashion to promote the exchange of information of interest to NCIS or to develop rapport with personnel who can provide tangible aid in the performance of the NCIS mission. The following conditions should apply:

a. The event is:

(1) Hosted in the name of NCIS; or,

(2) Co-hosted by NCIS with other agencies; or,

(3) Provided funds to sponsor attendees invited by NCIS. An example of this latter situation would be where a professional organization sponsors a function and provides a quota of invitations to NCIS for subsequent distribution. In such cases, all personnel invited to attend the function at NCIS expense must fit one of the categories of authorized attendees.

b. The function is a meeting to develop rapport with non-NCIS personnel (i.e., other LE/security officials) who are or expected to be in a position to provide information or services that will facilitate performance of the NCIS mission. Meetings that support specific operational events are not to be considered liaison.

c. A majority of attendees (or, NCIS invitees) must be non-DoD personnel.

d. Authorized attendees are limited to the following:

(1) Foreign government, foreign military, and foreign law enforcement personnel in a position to directly aid the NCIS mission (and, their spouses when appropriate).

(2) State and local government and law enforcement personnel in a position to directly aid the NCIS mission (and, their spouses when appropriate).

(3) Civilian personnel (U.S. citizenship notwithstanding) who are providing, or, who may be reasonably expected to provide, information or service of value to the successful completion of the NCIS mission.

(4) U.S. Government (including NCIS) personnel, only when official business or protocol clearly dictates their presence, provided that the number of DoD personnel does not exceed half the total attendees. For those events not hosted directly by NCIS, but for which NCIS shares the expense and is allotted a specific number of invitations for subsequent issue, the majority of the NCIS issued invitations must be non-DoD personnel. Under no circumstance should the number of DoD personnel constitute a majority of the personnel invited by NCIS and reasonably expected to attend the function.

(5) Attendees normally will be from within the geographical area serviced by the host NCIS activity. Use of EEE funds to pay for the travel of individuals invited to attend a liaison function is prohibited without prior authorization from DIRNCIS.

e. Limitations on expenses are as follows:

(1) Food, beverages, tips and service charges, room rentals, and decorations are all normal costs incurred for liaison functions. They should be commensurate with per person charges normally incurred within the geographical area in which the function is held. Alcohol consumption, when appropriate, must be maintained at a reasonable level by all attendees.

(2) Conference and registration fees for NCIS attendees (NCIS personnel or invitees) for overt participation in professional conferences and meetings are not authorized if other methods are available for payment of such fees.

(3) When multiple memento items are appropriate for presentation at a liaison event, they should be obtained from the bulk memento inventory at the parent field office or NCISHQ if available. Items similar to bulk mementos may be purchased at the time of the liaison event, and charged as a liaison expense. Attach a listing of memento recipients.

(4) Liaison expenditures (to include mementos purchased for the liaison event) must be approved in advance. Associated claims will specifically indicate when and from whom the required approval was obtained. Approval thresholds for liaison events are:

(a) Less than $1000 – SSA.

(b) Less than $2000 – ASAC or resident agent in charge (RAC).

(c) Less than $3,000 – SAC or DAD.

(d) Less than $5,000 – appropriate EAD, AD, or the DIRNCIS/Deputy Director.

(e) Up to $10,000 – DIRNCIS.

(f) More than $10,000 – Under Secretary of the Navy.

f. When completing NCIS Form 029 for liaison expenses the following information must be included:

(1) The purpose and location of the function.

(2) The approving official and when approval was obtained.

(3) The items or services purchased with the names of vendors/suppliers.

(4) A general description of the information, or, service gained, or, anticipated to be gained.

(5) A complete list of personnel attending, with their organization and title.

(6) If less than a majority of attendees were non-DoD personnel, then a complete explanation will be provided. Use a continuation sheet (plain piece of bond paper) if needed.

g. Expenses for high cost events with numerous expenditures should be consolidated on a single claim by the coordinator of the event or by the EEE fund custodian. In such cases, a single addendum may be attached to the claim with the information required above.

h. Events requiring authorization at the headquarters level or above should be submitted with a minimum of 45 days lead time to ensure proper staffing, review and approval.

i. If the claimant is in a travel status and receiving per diem for meals, then the cost of their meal consumed during the liaison event shall not be reflected on the claim.

37-9.2. Bulk Mementos. Bulk mementos are items purchased in numbers for future distribution to those authorized beneficiaries of EEE funds expenditures. See the requirements below regarding aggregate and unit cost issues. Authorized beneficiaries include liaison guests, operational assets, and other people authorized in this chapter. Presentations of bulk mementos must be made in the name of NCIS and not as a personal gift of the presenter. The value of bulk memento items presented to individuals will be commensurate with the level of information or service obtained from each recipient. Bulk mementos may not be provided to DoD employees unless the mementos are distributed to guests of a liaison event and the DoD employees comprise less than 50 percent of the invited guests.

a. Bulk mementos purchased with EEE funds may not be used for presentations for awards to government (Federal/state/local) personnel. In these instances, awards may be presented in accordance with reference (e) and applicable Government Accounting Office (GAO) Comptroller General opinions utilizing operation and maintenance (O&M) funds.

b. Typical bulk memento items include NCIS memorabilia such as lighters, pens, desk sets, cups, plaques, and other items bearing the NCIS logo.

c. Mementos purchased for specific, imminent events shall be considered a liaison expense. Any items still on hand after the event will be entered into the bulk memento system as provided for in this section.

d. Bulk memento purchases must be approved in advance. Approval thresholds for the purchase of bulk mementos apply as follows:

(1) Less than $1,000 – SSA.

(2) Less than $2,000 – ASAC or RAC.

(3) Less than $3,000 – SAC or DAD.

(4) Less than $5,000 – appropriate EAD, AD, or, the DIRNCIS/Deputy Director.

(5) More than $5,000 – DIRNCIS.

e. Specific claim filing instructions for bulk memento expenses are as follows:

(1) Block 9: provide a complete listing of the items purchased and the quantity and unit cost for each.

(2) Attach all receipts using continuation sheets (bulk memento expense claims must have receipts).

f. A bulk memento inventory log will be maintained for all items. The bulk memento log will account for transaction dates, identities of recipients, the number of items presented or purchased, the remaining inventory balance, and the NCIS official effecting the activity. If the unit cost of any bulk memento item is valued at $10 or more, the log book must be annotated to reflect the name and title of the authorized individual it was presented to and the date of presentation. If the unit cost of any bulk memento item is valued at less than $10, the identity of the NCIS employee who was issued the items is sufficient. Either a bound logbook or loose-leaf binder may be used. Appendix A provides an example of the approved bulk memento inventory log.

g. The bulk memento inventory log shall be retained for a period of three years, absent any discrepancies.

h. Bulk memento items will be kept under lock and key. A custodian will be appointed in writing and will be responsible for safeguarding the bulk memento locker, effecting distribution of bulk mementos and maintaining the required log. It is recommended that the bulk memento custodian not also be the EEE fund custodian.

i. There are financial restrictions limiting EEE expenses during the last two months of each fiscal year. Requests to purchase bulk mementos in August and September must be submitted to the Comptroller in advance of the transaction.

j. Inventoried non-perishable bulk mementos will be kept at a level sufficient to ensure requirements can be satisfied and will be purchased in economic order quantities. Inventories of perishable items will be maintained at a reasonable level commensurate with local requirements.

k. Bulk memento inventories will be inspected and reconciled at least annually by the EAD, AD, DAD, SAC, ASAC, FOSO, or SSA. The Comptroller will issue a general administration message reinforcing this requirement. Annotations of such inspections will be placed in the bulk memento inventory logbook. Each NCIS resident agency (NCISRA)/office having effected bulk memento transactions at any time during the preceding fiscal year will, by October 15th of each year, forward a copy of the bulk memento inventory log to the parent NCIS field office and headquarters department. NCIS field offices and headquarters departments will retain these inventories for three years. Retention of these inventory records is an annual office self-inspection and triennial IG inspection requirement.

l. Relief from discrepancies will only be approved in accordance with the provisions of reference (f). Discrepancies will be fully investigated by the SSA (not to be delegated) and resolved as follows:

(1) For discrepancies not exceeding $25, the inventory log will be annotated with an adjusting or explanatory entry and signed by the SSA.

(2) For discrepancies not exceeding $50, the SSA based on the written authorization of the SAC will annotate the inventory log. Such authorization will be noted on the corresponding page(s) in the bulk memento inventory log.

(3) For discrepancies exceeding $50, a complete report will be forwarded via the parent NCIS field office to the IG for subsequent review. Relief of liability from the responsible personnel will be contingent on the written concurrence of NCISHQ.

37-9.3. Operational

a. Expenses that are required to advance the objectives of a specific investigation or operation will be charged to this category.

b. Expenses for food, beverages, tips and service charges, hotel/motel fare, and similar costs may be claimed under this category when they are associated with maintaining operational security or are necessary elements of the source handling process.

(b)(7)(E)

d. Wherever feasible, expenses for parking, tolls, and use of privately owned vehicles (POV) pursuant to operational contacts will be claimed on Standard Form 1164 (SF 1164), Claim for Reimbursement for Expenditures on Official Business, unless the existence of such documents would jeopardize the security of an ongoing case or person supporting the NCIS mission.

e. Persons on TDY will include only amounts that exceed per diem entitlements. The sub-voucher shall include details of the adjustment.

f. Types of operational expenses can include, but are not limited to:

(1) Contacts. Operational contacts are defined as meetings with non-NCIS personnel to obtain information of interest to the NCIS mission or to cultivate the individual(s) for future utilization as an asset for such information. (b)(7)(E) When operational security dictates that such meetings be held away from the NCIS office, then reasonable expenses pursuant to conducting the meeting at another location may be reimbursed with EEE funds. Expenses for meetings held with other law enforcement officials (with the exception of U.S. Federal law enforcement officials/employees of the U.S. Government) for the purpose of discussing a specific case or operation fall within this category. Care should be taken not to confuse this operational category with liaison meetings.

(2) NCIS Asset Management System Expenses

(a) Reimbursements to assets will be reasonable and commeasurable with the value of the information obtained or reasonably expected to be obtained. Consult reference (g) for further guidance on the handling of assets.

(b) EEE funds may be used to reimburse assets for expenses incurred pursuant to the execution of specific NCIS tasking. Typically, these expenses will include food, beverages, use of personal vehicles, etc. Costs incurred for the purpose of personal security (i.e., rental of a secure facility or motel room) may also be charged to EEE funds if specifically authorized in advance by the asset's NCIS point of contact. Travel away from the assets home area, when authorized, may also be paid with EEE funds (see Travel section below). Care should be taken not to violate the prohibitions on dual compensation of DoD personnel as discussed in section 37-5.g. Asset expenses will be reimbursed only to registered NCIS assets, or persons reasonably expected to be registered within the imminent future.

(3) Travel

(a) On occasion it is necessary for NCIS or non-NCIS personnel supporting the NCIS mission to travel on special missions in a (b)(7)(E) TDY orders or invitational travel orders (ITO) will be used in these instances whenever possible. However, when submission of travel documents outside NCIS would jeopardize the security of the individual or the NCIS operation, the use of EEE funds is authorized. The limitations on expenses for TDY orders established by the Joint Travel Regulations (to include current per diem rates) will be used as a guideline for the EEE traveler. In those cases when per diem rates are exceeded, approval is required from the DIRNCIS, Deputy Director or respective AD. In addition, written approval from Legal Counsel is required to ensure compliance with references (a) and (h).

(b) Tickets, receipts, and associated documentation in these instances should not indicate an affiliation with NCIS. If such affiliation is indicated, then there is no justification for the use of EEE funds for travel. The only exception to this provision is when such reference constitutes an inadvertent compromise and the EEE submission is used solely to limit the extent of that compromise.

(c) Some examples of authorized EEE travel are:

1. Travel by NCIS personnel in a UC capacity outside of their normal area.

2. Travel by non-NCIS personnel in support of NCIS operations.

3. Travel by assets for personal security reasons and similar instances.

g. Constant Visual Surveillance

(b)(7)(E)

(2) Reimbursement of such costs is authorized when NCIS personnel, in a (b)(7)(E) VS status, must make purchases in order to avoid bringing themselves under suspicion (i.e., bar or restaurant expenses while maintaining CVS of an individual or area pursuant to an active NCIS case or operation, or while conducting general surveillance activity). Such personnel may also be reimbursed for meals consumed during CVS but only when the individual's freedom of choice as to when, where, and what to eat is significantly limited or dictated by operational requirements. The mere act of being in an overtime status is not justification for consuming meals at government expense.

(3) When in travel status, if a lunch or dinner meal is paid for by the sponsor of an event, attendees must reduce the per diem claim on their travel voucher by the amount allotted for that meal.

(4) The subject of the surveillance will be noted, if not the same as indicated in Block 3 of NCIS Form 029.

(5) Personnel on travel in support of CVS and who incur expenses for meals or lodging will reduce the amount claimed under EEE by the per diem allowance provided, with an explanation.

(6) When an operation is conducted at NCIS request in concert with other agencies and includes joint surveillance activity, expenses may be incurred by NCIS personnel for members of the participating organization. Such expenses, however, should be kept to a minimum consistent with operational requirements and the level of cooperation and/or support provided by the participating organization. In no case should expenses be incurred under this category for the sole purpose of entertaining the personnel of another agency (see the provisions regarding liaison expenses).

h. Emergency Purchases

(1) Even under the most carefully planned conditions, situations occur which require the immediate purchase of items necessary to support an investigation or operation. Although these items may be normally stocked or procured through official channels, foresight may not have led to having them available at the exact time they were needed and delaying the purchase would jeopardize the case or operation. In such cases, purchases with EEE funds under the operational category are authorized. Care should be taken, however, to plan all operations in advance to avoid necessitating such expenses.

(2) Typically, these expenses will include consumable items such as batteries, adhesive tape, evidence collection/storage equipment and other such expendable items. Only the amount required for the situation at hand will be purchased. Excess purchases will be disallowed, if not fully justified.

(3) Vendor receipts will be obtained whenever possible. However, care should be taken not to jeopardize operational security in this regard. Receipts that may be directly or indirectly tied to the asset (i.e., those which reveal the asset's name or association with NCIS) will be retained in locally maintained asset dossier, with an appropriate explanation. Claimants may also delete compromising information on the vendor receipt.

(4) Justification for use of EEE funds vice submission of an SF 1164 will also be provided in Block 9 if POV parking, tolls or other such expenses are included in the claim.

37-9.4. Protective Operations

a. Protective service operations (PSO) will be conducted in accordance with current guidelines and expenses incurred provided in the operational expense category. Typically, such expenses will include food and beverages, tips and service charges, and certain types of local and TDY travel expenses. Reimbursement for alcoholic beverage expenses consumed by members of a protective detail are not authorized under any conditions.

b. PSO support shall be coordinated with Protective Operations Field Office (POFO), in accordance with reference (i) and specifically funded by POFO. Normal expenses incurred during advance inspections and activities of a PSO are authorized for reimbursement; if reimbursement is sought from POFO the expenses must be approved in advance by POFO. In these instances, expenses will be claimed immediately upon completion of the PSO mission.

c. Personnel may also be reimbursed for meals consumed only when the individual's freedom of choice as to when, where, and what to eat is significantly limited or dictated by operational requirements. The mere act of being in an overtime status is not justification for consuming meals at government expense.

d. Specific claim filing procedures for expenses are as follows:

(1) Explain completely the reason for the expense, by whom and where it was incurred, and list all personnel (NCIS and non-NCIS) for whom the expense was incurred.

(2) Indicate on the sub-voucher if the event was coordinated by POFO.

(3) Note the principal of the protective operation.

(4) Reduce the amount claimed under EEE by the per diem allowance provided for lodging or the particular meal (breakfast, lunch, or dinner) consumed by personnel on TDY orders who incur expenses for meals or lodging. Block 9 should be appropriately annotated to reflect the deduction of the allowable per diem costs under TDY orders.

(5) Each individual expense requires its own sub-voucher, unless multiple expenses at a single establishment can be combined onto one sub-voucher. At the end of the PSO mission, the professional support assistant (PSA) or detail leaders shall collect all sub-vouchers for review and supervisory signature and submit them to the funds custodian for reimbursement.

(6) EEE expenses shall be reported on the Category 9A ROI submitted to POFO upon completion of the mission(s).

37-9.5. Non-Consumed Equipment

a. In support of emergent investigative or operational requirements, equipment such as laptop computers, cameras, binoculars, global positioning systems (GPS), personal data assistants (PDA) and storage/transport containers etc., may be purchased using EEE funds when either timeliness or operational security considerations preclude the use of the traditional requisition process. For accountability purposes, items meeting the thresholds in reference (j) must be entered into the Defense Property Accountability System (DPAS) or the alternate property accountability system used for classified or sensitive equipment. See reference (k) for descriptions of applicable property accounting systems.

b. Vendor receipts will be obtained whenever possible. However, care should be taken not to jeopardize operational security in this regard. (b)(7)(E)

(b)(7)(E)

d. The sub-voucher shall describe the intended disposition of any purchased equipment after the immediate need passes.

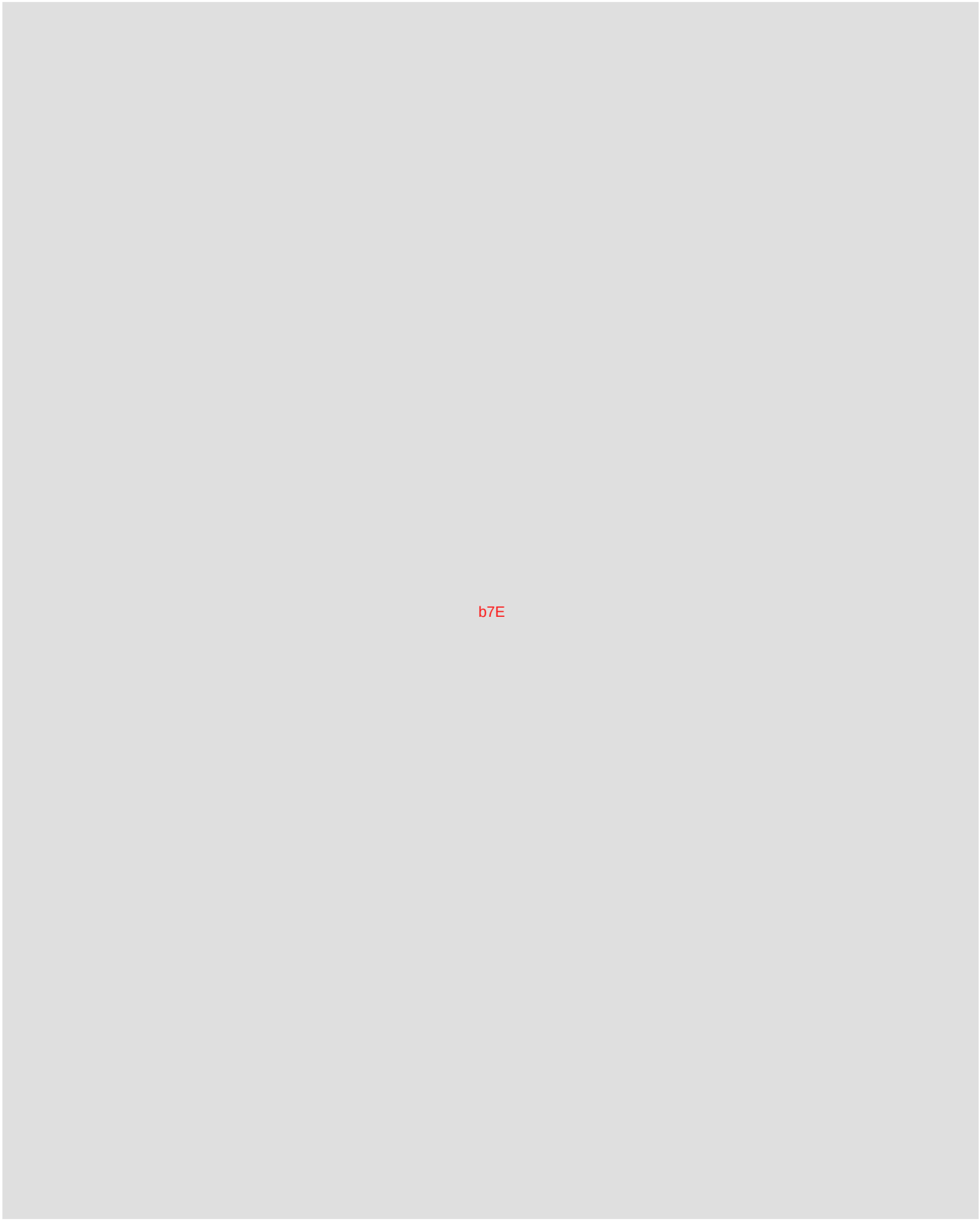
37-9.6. Undercover

a. When NCIS personnel are acting in a deep UC capacity pursuant to an ongoing case or initiative operation, (b)(7)(E) may be reimbursed with EEE funds. This authorization is limited to those expenses for which reimbursement through other means would (b)(7)(E)

b6, b7C

c. Personnel serving in deep UC roles and traveling under EEE funds (TDY orders not issued) are not subject to the limitations of per diem allowances. They are, instead, required to provide statements of actual expenses. In all instances, such expenses will be limited to those that are reasonable and necessary to the successful performance of the UC mission.

d. When filing a claim for UCA expenses, Block 9 will be annotated to indicate that the expense was incurred pursuant to maintaining a deep UC role, along with a justification for use of EEE vice other funds.


b7E

(2) Include in Block 9 a statement regarding the nature of the information or service obtained from the recipient of the payment.

(3) If approval above the NCISRA level was required, indicate by whom and when it was provided.

b7E

(b)(7)(E)

37-9.9. Evidence

a. One of the primary uses of EEE funds is for purchasing evidence during an active investigation or operation when no other legal recourse exists to obtain the required evidence, or, when the use of such means (i.e., subpoenas or search warrants) would jeopardize the security or further potential of an ongoing NCIS case or operation.

b. Typical evidence expenses include the purchase of narcotics, computer media, stolen property, classified material, and other items necessary to perform an investigation regarding the item/material purchased.

c. EEE funds may not be used for the purchase of evidence not directly related to an ongoing NCIS case or initiative operation. For this reason, no evidence purchase utilizing EEE funds will be made in the absence of an established case control number (CCN), unless the establishment of such is imminent.

(b)(7)(E)

(b)(7)(E) Approval thresholds may be delegated to subordinate management personnel, but such delegation must be written. All associated EEE claims will indicate specifically from whom and when approval was obtained in Block 9 of NCIS Form 029. The following thresholds apply:

(1) Less than $1,000 – SSA.

(2) Less than $2,000 – ASAC or RAC.

(3) Less than $3,000 – SAC or DAD.

(4) Less than $5,000 – EAD or AD.

(5) The DIRNCIS must approve payments in excess of $5,000.

e. Specific claim reporting procedures for the purchase of evidence are as follows:

(1) A detailed description of the item purchased will be annotated in Block 9.

(2) The evidence log number assigned to the item/material will be indicated. If evidence purchased with NCIS funds is being retained in another agency evidence facility, the assigned log number will be indicated.

(3) The evidence log number assigned to recovered funds, if any, will also be annotated.

(4) Subsequent disposition of the evidence, if known, will be fully described. This is especially important for instances where joint operations with other agencies result in NCIS purchased evidence being retained by another agency or organization. Maximum detail should be provided to the extent possible.

37-9.10. Miscellaneous

a. It is occasionally necessary to incur expenses that cannot be suitably charged to one of the specific categories listed above, but which for confidentiality purposes the use of EEE funds is appropriate. Such expenses will be limited to those that cannot be affected through the use of some other appropriation and which, if not affected, will jeopardize specific NCIS operations, personnel, or persons of interest. The use of this category will be minimized.

b. Miscellaneous purchases for material or services that support a specific case or operation will use the operational expense category. Only use this category if there is no open or active investigation or operation.

c. Claims filed under this category will be annotated with a complete justification for using EEE funds, the ramifications had the expense not been incurred, and a description of the item or service obtained.

37-10. Special Incidents of Use of EEE Funds

37-10.1. Procedures for Group (I) Operations

a. Initiative criminal operations meeting specific criteria as set forth in reference (m) are considered Group (I) operations. Due to the sensitive nature of the investigative techniques utilized, all Group (I) operations require NCISHQ approval and funding. Accordingly, all Group (I) funding is administered and monitored by NCISHQ Criminal Operations Division.

b. Funding for Group (I) operations will be controlled by NCISHQ. The case control office will submit an operational proposal outlining the amount of funds required for the operation, projected expenses (quarterly) to be incurred, and identify an individual at the field office to be the designated fund custodian (DFC), who is separate from the EEE fund custodian and EEE paying agent, and will administer the specifically designated fund and be responsible for sub-vouchers (NCIS Form 029) and filing claims (NCIS Form 030) applicable to the operation. NCISHQ will approve or amend the funding request. Once funding is authorized, the case control office and field office will be notified. An advance may be requested by the DFC to the appropriate EEE fund custodian or paying agent.

c. The DFC may open an office account (non-interest bearing) at a suitable bank for cashing or depositing the advance check and any reimbursement checks. This will allow offices receiving substantial advances to cash the check, deposit a portion of the funds in the account if desired, and maintain a cash box. This account will be used for official purposes only and will be closed upon termination of the operation. If activated, a copy of the monthly bank statement will be forwarded to NCISHQ Criminal Operations Division.

d. The DFC may cash the check and maintain the total advance and any subsequent reimbursement in the cash box. The cash box will be administered in the same manner that a fund custodian or paying agent maintains a cash box. The NCIS field office SAC or designee will conduct monthly verifications of the entire advance. These monthly verifications will be unannounced and conducted on a random date selected by the verifying official. The DFC will maintain a ledger that records funds authorized, advanced, expended and remaining.

e. The DFC will prepare and submit the appropriate NCIS Form 030 monthly via the normal field office chain of command.

f. Under no circumstances will expenses exceed the authorized funding approved by NCISHQ Criminal Operations Division. A request for additional authority may be submitted via an ROI.

g. NCISHQ Criminal Operations Division personnel may periodically conduct an onsite visit to assess the operation and conduct an audit of the funds.

h. Funds are issued by fiscal year. If an investigation or operation spans two fiscal years, a new request for authority is required. Thirty days prior to the end of the fiscal year the DFC will provide to Criminal Operations Division the balance of funds remaining and projected expenses for the final month of the fiscal year.

i. Joint Group (I) UC operations that request a lump sum transfer of EEE funds between two agency headquarters (e.g., NCIS to Federal Bureau of Investigation (FBI)) will be facilitated/administered by NCISHQ Criminal Operations Division and the Comptroller. NCISHQ Criminal Operations Division will submit an NCIS Form 028 to the NCISHQ EEE paying agent. NCISHQ Special Operations Division will then forward a check via registered mail to the participating agency's headquarters. NCIS Form 029 will then be submitted with a copy of the check and return receipt as addendums. A record of expenditures will be provided by the participating agency.

(b)(7)(E)

37-10.2. Credit and Debit Cards Issued for UC Personnel

(b)(7)(E)

b7E

37-10.3. Training Events

a. Certain training events, for purposes of realism, require the participants to incur expenses that may not be reimbursed through the use of a SF 1164 or SF 182 (Authorization, Agreement and Certification of Training (For DoD Use Only), or other means. Absent these means, expenses may be charged to EEE Funds.

b. Typical expenses will include admission fees, meals, tips and service charges, and hotel/motel charges (when approved in advance by appropriate authority). The expense must be one that was absolutely necessary to the conduct of the training event in order to be claimed from EEE funds. For this reason, absolutely no alcoholic beverage charges (including those incurred by the acting principal) may be reimbursed under this category.

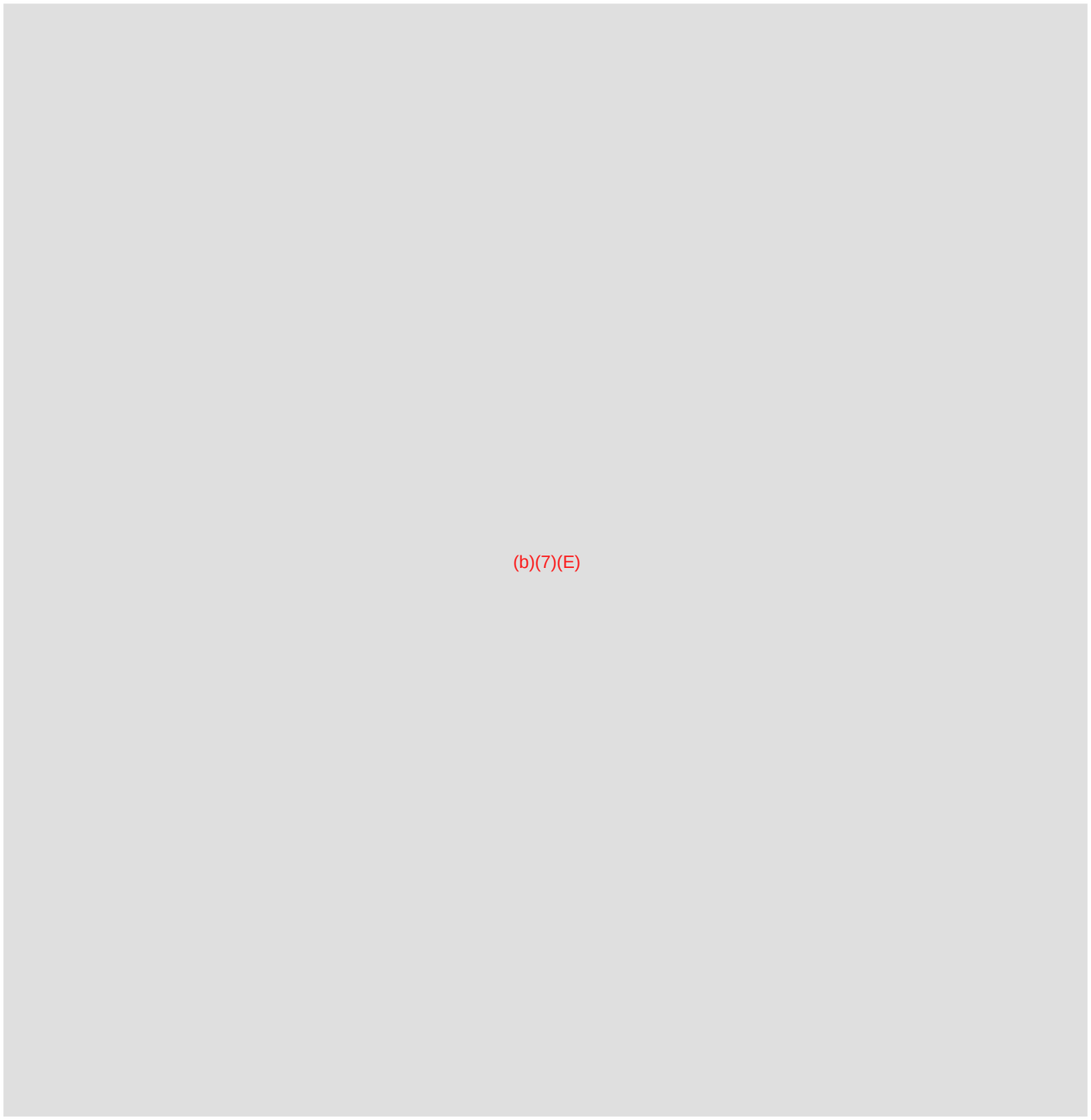
c. If a claimant is unsure as to whether an expense is allowable under SF 1164 procedures, then the servicing personnel support detachment/unit should first be consulted. If that office subsequently disallows such a claim, then it may be reimbursed after the fact from EEE funds.

d. Specific claim filing procedures for training events are:

(1) Use the miscellaneous expense category; and.

(2) Annotate clearly in Block 9 that the expense was incurred for training purposes.

(b)(7)(E)



37-10.5. EEE and Other Funds Held in Evidence

a. As noted in section 37-9 EEE funds can be subsequently recovered and logged in as evidence. Once proper disposition authority has released the funds from evidence, the Comptroller must return it to the U.S. Treasury. All such funds must revert to the U.S. Treasury via the following procedures:

b. The evidence custodian will return the funds to the fund custodian at the parent NCIS field office by obtaining a check made payable to "DFAS-CL 8522". The field office EEE fund custodian will forward the check to the NCIS Comptroller's office. The check and cover letter will identify the evidence log number, case/operational title and CCN and state that the check represents recovered EEE funds.

c. Non-EEE Funds held in evidence and subsequently released will be treated in the same manner, except that the check or cover letter will indicate that the funds were seized and are being reverted to the U.S. Treasury.

d. Funds that are generated from UC employment activity of NCISHQ personnel will also be treated in this manner. Payroll checks will be cashed by the UCA and the funds submitted to the EEE fund custodian at the NCIS field office, who will then process them in the same manner as any other non-EEE funds.

e. The Headquarters Accounting Officer will prepare an appropriate cash collection voucher (CCV).

f. For recovered EEE funds, the CCV will be credited to the same account as the year in which originally expended. If the evidence funds are returned within the current fiscal year, contact the Comptroller's office to obtain appropriate instructions to adjust the memorandum accounting records at the local level. This action will in effect permit the reutilization of these funds.

g. For non-EEE funds, the CCV will be clearly annotated as miscellaneous funds being reverted to the U.S. Treasury "Conscience" Fund. Under no circumstances will non-EEE funds held in evidence or generated during UC operations be credited to EEE balances.

h. Additional information regarding the disposal of currency that has been retained in the NCIS Evidence Custody System can be found in reference (n).

37-10.6. Foreign Currency Conversion

a. The gain or loss in any foreign currency conversion will not be borne by NCIS personnel. Applicable field offices will establish and disseminate procedures for ensuring that such transactions are accounted for. Receipts for conversions of funds will be retained and appended to NCIS Form 029. Absent a receipt, the circumstances involving the conversion will be explained.

b. When filing claims for EEE expenditures involving the use of foreign currency, the following minimum provisions apply:

(1) Only U.S. dollar values will be used in Blocks 4 and 12 of NCIS Form 029.

(2) Costs associated with obtaining the foreign currency and converting any remaining currency back to U.S. currency will be included as part of the cost of incurring the underlying expense.

(3) Block 9 will be annotated to clearly indicate the amount of foreign currency expended and the rate at which the U.S. funds were originally converted to foreign currency. In cases where an advance was provided to the claimant in foreign denominations, the fund custodian will advise the claimant of the appropriate conversion rate. In cases where dollars were converted into foreign currency at different exchange rates, the cited rate will be the one at which the majority of the funds were converted.

(4) If the claimant was responsible for conversion of funds, then conversion documents will be appended to the ensuing claim. Any absence of these documents will be fully explained in Block 9 to NCIS Form 029.

37-10.7. Sales Tax on EEE Expenditures

a. Federal funds, including EEE funds, are not subject to jurisdictional taxing authority within the United States. However, it may not always be prudent or possible to provide tax-exempt certification to a vendor when incurring an expense due to operational security requirements.

b. When an overt EEE purchase is affected, disbursing personnel should attempt to avoid the payment of sales tax. Many vendors will forego such payment upon presentation by the purchaser of a valid form of U.S. Government identification (i.e., NCIS badge or credentials). Others will honor the request if provided with a written certification of tax exempt status. The EEE fund custodian will maintain these certificates for issue to NCIS personnel as required. NCIS personnel are encouraged to affect EEE expenditures with vendors who honor the tax-exempt status of such purchases. However, NCIS personnel should use prudent judgment when effecting purchases in this regard. These paragraphs should not be interpreted as reason to jeopardize the security or confidentiality of an ongoing NCIS case or operation or person of interest.

37-11. Cash Handling Positions

37-11.1. Paying Agents

a. Paying agents, formerly called agent cashiers, administer EEE funds, provide advances to authorized personnel and perform selected accounting functions for those funds. Paying agents will be appointed as required by the Comptroller and may support one or more field offices.

b. Reference (o) specifically authorizes NCIS to designate paying agents to perform those duties as assigned within this chapter. The original of this authorization is held by the Comptroller should any controversy arise when dealing with local disbursing officers.

c. Designated paying agents will be appointed in writing by the Comptroller and maintain an advance of EEE funds. Appendix B provides information for completing a DD 577, Appointment/Termination Record – Authorized Signature form. The paying agent will maintain the funds in a checking account at a qualified banking institution.

(1) Consideration should be given to using an interest bearing account. When establishing the checking account the paying agent should evaluate the cost of an interest bearing account (i.e., charges for deposits, checks and cashier checks) as compared to a non-interest bearing account. An interest bearing account should be the one of first choice, unless there is a significant increase in bank charges associated with such an account. When an interest bearing account is established, interest earned should be paid to the U.S. Treasury annually or whenever the amount exceeds $100 via a check made out to the "DFAS-CL 8522" and sent to the NCIS accounting officer.

(2) The paying agent will use checks drawn against this account to advance funds to NCIS field office fund custodians and other authorized personnel. Section 37-12 provides details on obtaining advances.

(3) The paying agent's checking account should be used for effecting all receipts and disbursements of EEE funds. Where necessary, paying agents are authorized (at personal risk) to maintain a reasonable amount of cash on hand, but no more than is deemed absolutely necessary for meeting emergency, time-sensitive needs. When cash is retained on hand, it will be kept in a container secured by a combination lock as provided for by reference (f). That container will not be used for storing any other items of value. Safe combinations will be changed every six months.

d. Paying agents will ensure that cash advances that they have issued are reconciled and recouped (when appropriate) in a timely fashion. Annual reviews of all revolving advances will be performed during September to ensure that they comply with the guidelines provided in section 37-12. Records of these reviews shall be retained for one year.

e. Upon receipt of NCIS Form 030 from fund custodians and other authorized personnel, paying agents will issue a replenishment check in the amount claimed on the forms to the submitting individual.

f. A verification of assets will be performed monthly in accordance with the procedures set forth in section 37-15.

g. To replenish the paying agent's account at a field office, a Voucher for Confidential Expenditures (DD Form 281) will be prepared by the paying agent, signed by the paying agent as "Payee" and, signed by the SAC or designee as "Certifying Officer." To replenish the paying agent's account at NCISHQ, DD Form 281 will be prepared by the paying agent, signed as "Payee" and signed by the Comptroller as "Certifying Officer".

(1) The original form will bear an annotation that supporting documents are held on file at NCISHQ for review and audit purposes. It will be submitted to the servicing disbursing office. Any other documentation required by the disbursing office will also be prepared.

(2) A copy of the form (completed and annotated with a Disbursing Office Voucher Number (DOV)), will be submitted along with all original NCIS Forms 030 and 029, to the Comptroller.

(3) Amounts claimed on the form will represent the total EEE funds expended under the appropriate subhead.

(4) The Comptroller will issue appropriate accounting data for inclusion on the form.

(5) Upon submission of the original form to the appropriate disbursing officer, the paying agent will be issued a replenishment check for deposit to the EEE checking account.

h. Paying agents will maintain such records as directed by the local DON Comptroller, Navy Comptroller (NAVCOMPT), and other authority. When nearing or meeting the limit of the NCIS field office's EEE authorization, the paying agent will initiate steps to obtain an increase in the authorization. EEE expenditures should not exceed the authorized amount.

i. Paying agents and others involved in the execution of EEE funds must have a clear understanding of the relationship between EEE advances and the operating target (OPTAR) issued by the Comptroller.

j. Additional guidance for specific questions which may arise in the handling of cash which is held by paying agents or fund custodians may be found in reference (f) volume 5, "Disbursing Policy and Procedures."

k. EEE funds and associated documentation will be kept in a safe that meets the minimum requirements for storage of currency and negotiable instruments as prescribed in paragraph 030304 of reference (f), volume 5. Safe combinations will be changed every six months.

37-11.2. Fund Custodian

a. Fund custodians hold revolving advances at personal risk from which they issue cash to subordinate fund custodians and individual NCIS personnel for EEE advances or reimbursements. Funds custodians are reimbursed by submitting claims to the appropriate paying agent.

b. Appointment of EEE fund custodians (to include field office and other subordinate fund custodians) will be made in writing. A copy of the appointment will be provided to the designated paying agent. Appendix C provides information for completing a DD Form 577, Appointment/Termination Record – Authorized Signature form appointment authorization.

c. Advances issued to fund custodians will be limited to the minimum required to satisfy normal requirements. Additional one-time advances may be requested to accommodate unique situations that arise. Section 37-12 provides guidelines for the normal amount to be advanced.

d. A verification will be performed monthly in accordance with the procedures set forth in section 37-15.

e. EEE funds and associated documentation will be kept in a safe that meets the minimum requirements for storage of currency and negotiable instruments as prescribed in paragraph 030304 of reference (f), volume 5. Safe combinations will be changed every six months.

f. Only the funds custodian shall have access to the funds and other assets comprising the advance. Alternate fund custodians shall not be appointed. Fund custodians may sub custody their funds in total to another during extended absences.

37-11.3. Advance Holders

a. An "advance holder" includes paying agents, fund custodians and any other person who holds EEE funds. Anyone receiving an advance must be familiar with this chapter's contents.

b. There are two categories of advances.

(1) Revolving – Required for an indefinite period of time. Normally this category of advance is limited to paying agents and fund custodians. Other situations exist where an individual holds a revolving advance due the unpredictable nature of their duties or their geographical separation from the office. Examples include agents afloat, storefront operations and special operations squads. All advances subject to monthly verifications, similar to those required of fund custodians.

(2) One-Time – Required for a specific event with a finite termination date. One-time advances should be requested only shortly before needed. Expenses should be reported within five days of occurrence and any remaining advanced funds returned also within five days.

c. NCIS personnel who have been issued advances are personally liable for the proper safekeeping of the funds and shall be able to account for the full amount at all times. When the need for an advance has expired, it will be liquidated. Unlikely or infrequent contingencies will not serve as the basis for retaining an advance, either one-time or revolving.

37-12. Advances

37-12.1. Obtaining an Advance

a. Advances will be issued through the submission of a "Request for Advance of EEE Funds" (NCIS Form 028). A blank request is contained at Appendix D.

b. The type of advance (revolving or one-time) must be clearly indicated. Case control numbers are not required on NCIS Form 028 unless the advance is requested pursuant to a specific operation being tracked at the field office or NCISHQ level (including protective operations). However, a clear statement of intended use will be provided. Amounts requested must be consistent with the intended purchase. Submit requests as soon as the need is identified to give the issuing activity sufficient time to make suitable arrangements. Actual issuance of the funds should be as near as possible to the date needed.

c. Requests for all revolving advances and one-time advances exceeding $2,000 require the approval of the SAC or DAD. Other one-time advance requests may be approved by an SSA or above. Under no circumstances will a person subordinate to the requester act as the approving official. Also, in no instance will the requesting agent or fund custodian approve an advance.

d. Once approval has been obtained, the requester will submit NCIS Form 028 to the fund custodian or paying agent (as appropriate) as follows:

(1) If submitted in person, the cash receipt certificate section will be completed by the fund custodian or paying agent and signed by the requester. The fund custodian or paying agent will retain the original until the advance is liquidated.

(2) If submitted by fax or e-mail, the requestor will sign Cash Receipt Certificate portion prior to submission. The fund custodian or paying agent will complete their portion and return it to the requester along with a check drawn from the checking account. The requester will forward the original form to the fund custodian or paying agent. Under no circumstances will NCIS personnel cash an advance check without first returning the completed form.

e. EEE fund custodians and paying agents will maintain a manual or automated log of outstanding advances. The log will contain, at a minimum, the following information:

(1) Name and duty station of person to whom funds were advanced; and,

(2) Date that funds were advanced; and,

(3) Amount of advance; and,

(4) Estimated liquidation date (not required for revolving advances), and,

(5) Actual date of liquidation (when liquidated).

f. Liquidation will be effected by the return of cash in the amount of the original advance, submission of NCIS Form 029 for the entire amount advanced or a combination of both.

g. Upon liquidation, the EEE fund custodian or paying agent will complete the liquidation information on the NCIS Form 028, provide the original to the requester and retain a copy. The log will be annotated to indicate liquidation in full has occurred.

h. When a revolving advance needs to be adjusted, the requester will complete a new NCIS Form 028 for the revised amount. A pen and ink change to an advance is only permitted while the adjustment is being made. The old advance form will be liquidated.

i. When the local fund custodian cannot satisfy a request for advance, the request will be forwarded to the next level custodian or the paying agent.

j. Written requests may be preceded telephonically for coordination and confirmation that funds are available, but the actual issuance of funds is not to be accomplished without a properly approved request. An advance faxed or scanned/e-mailed copy is acceptable to receive an advance, but must be followed by the signed original request.

37-12.2. Determining Amounts to be Advanced

a. NCIS field offices are authorized a revolving advance as determined by the Comptroller. The amount authorized will be based on monthly expenses and field office size and complexity.

Field office advances will be reviewed by the Comptroller's office annually to ensure that excessive and/or insufficient advance balances are avoided. One time advances will be issued to handle unique finite-term events.

b. The amount of funds to be advanced to an individual NCISRA will be determined by each field office, though NCISHQ review of the overall field office advance will have a bearing. As a guideline, an amount up to twice the average total monthly EEE expenditure is recommended. Distance from the fund custodian is also a key factor. Deviations are authorized at the field office discretion, but must be validated annually.

c. The overriding factor for determining the size of a revolving advance is the expectation that expenses are submitted and reimbursed at least monthly. Offices that have a history of less frequent submissions shall not have an advance that allows for this tendency. Infrequent multiple submissions within a month due to unusually high expenses are not considered cause for a permanent increase in the revolving advance.

d. Special agents afloat (SAA) should be provided a revolving advance based on the ship's projected deployment schedule. A $500 advance while home ported and $1,000 when deployed is recommended.

37-13. Filing Claims

37-13.1. Sub-vouchers

a. Individual claims for the expenditure of EEE funds will be filed on the Sub-voucher for Disbursement of EEE Funds (NCIS Form 029). Sub-vouchers may be submitted for the reimbursement of personal funds expended for official purposes or as a liquidation of an outstanding advance of EEE funds. All NCIS Form 029 will be typed.

b. Under normal circumstances it is expected that NCIS Form 029 will be submitted to the fund custodian for payment within five days of the expenditure. Generally, the individual who actually spent the funds will submit NCIS Form 029, once approved by their supervisor as a valid expenditure, to their respective fund custodian.

c. In cases such as deep UC roles, the controlling agent may submit NCIS Form 029 on behalf of the UCA.

d. Specific, line-by-line instructions for NCIS Form 029 are provided in Appendix E. Requirements for each specific expense category are provided in section 37-9.

e. In spite of deployments, the SAA is expected to submit expenses monthly. They may submit sub-vouchers and receive reimbursement at any field office, regardless of where they received their advance. When the deployed ship is operating within a particular field office's area of responsibility, submission of sub-vouchers to that field office is the preferred method.

37-13.2. Claims

a. NCIS Form 030 is used to consolidate sub-vouchers, obtain upper level management approval of the expenses and request reimbursement.

b. Fund custodians, paying agents, and such other persons, as occasionally directed, are responsible for preparing the claim and submitting it through the appropriate approval process.

c. Fund custodians and paying agents are responsible for monitoring their advances and reporting the outlay of funds. Compliance with the guidance provided in section 37-9 is the responsibility of supervisory and management personnel.

d. Line by line instructions for NCIS Form 030 are provided in Appendix F. Claims should be submitted at least monthly. Negative reports are required.

e. To prevent a conflict of interest or perception of impropriety, a claim (NCIS Form 030) must not contain any sub-vouchers (NCIS Form 029) that has been submitted by the approving official.

37-14. Fund Administration

a. The NCIS Comptroller's office provides EEE fund administration services to NCISHQ and NCISFOs. Normally, Operating Targets (OPTARs) will be issued to each field office on a quarterly basis.

b. OPTARs are issued on the basis of requirements, historical utilization, and anticipated needs. Each OPTAR holder is responsible for ensuring efficient utilization of the funds provided. Requests for additional funding should be submitted to the Comptroller in advance of exceeding existing funds. Unlike regular operating funds, managing EEE funds to limit spending within an OPTAR ceiling or to reach an OPTAR goal is not expected or recommended.

c. Excess balances may be recouped for redistribution as required. Periodic calls for identification of excess balances may be requested.

d. No more than 20 percent of the total EEE OPTAR may be expended in the final two months of the fiscal year without written authorization from the Comptroller.

37-14.1. Obligation Reports

a. Paying agents will prepare and submit a report on the 25th day of each month of expenses to the Comptroller, or, his designee, via fax or e-mail with file attachment. The report requires the following information:

b. Total expenses for the month and fiscal year-to-date, using the following codes:

	Law Enforcement	Counterintelligence
Liaison	LE1	CI1
Bulk Mementos	LE2	CI2
Rewards	LE3	CI3
Operational	LE4	CI4
Protective Operations	LE5	CI5
Non Consumed Equip	LE6	CI6
(b)(7)(E)	LE7	CI7

Evidence Purchases	LE8	CI8
(b)(7)(E)	LE9	CI9
Miscellaneous	LE10	CI10

c. The funding status of any Group I operation.

37-15. Cash Verification

a. In all situations, whenever verification is conducted the form certifying the verification shall be forwarded to the person that issued the underlying advance. The verification of the paying agent shall be forwarded to the Comptroller. Records of verifications shall be retained until the next IG inspection.

b. The term "verification" covers all assets that comprise the total of the advance, such as cash, sub-vouchers, claims, checks, etc.

c. The first step in any verification is to sight the advance holder's Request for Advance of EEE Funds to determine the total amount held.

d. Individuals tasked with performing verifications should have a thorough understanding of this section. Trusting the advance holder to ensure that the verification is properly done defeats the purpose of this important internal control.

e. Verifications will be conducted on a monthly, unannounced basis by a responsible official (SAC, ASAC, SIO, FOSO, SSA, SPA, etc.) or disinterested third party designated by such official. The cash verification will be conducted on a randomly chosen date and not coincidental to the submission of NCIS Form 030.

37-15.1. Verification of Revolving and One-Time Advances

a. Every revolving advance of EEE funds, with the exception of those issued to the SAA and/or geographically isolated offices, and one-time advances held for longer than a month will be subjected to cash verification at least once every calendar month. During verification, all financial assets will be inventoried to ensure that the full advance is present. The verification will be performed by an individual at least one supervisory level above the revolving advance holder.

b. Though it is a supervisory responsibility for the monthly verification of assets, the actual revolving advance holders are equally responsible for ensuring that verification is done each month.

c. A manual verification form is contained in Appendix G. Automated forms that reflect the same information are acceptable.

d. Monthly verifications of SAA advances are not required during deployments away from the homeport. A full verification will occur upon return. For this reason, it is important that sub-vouchers submitted from SAA personnel be carefully reviewed. Monthly "Negative Expenditure Reports" are also recommended. Field offices and NCISRAs at the deployed location can be asked to conduct verification if desired.

e. Verifications of revolving advances held at geographically isolated one-person offices should be conducted during supervisory site visits. In those offices staffed by two or more individuals a subordinate person may perform a monthly verification.

37-15.2. Verification of Paying Agents

a. In addition to this guidance, the disbursing officer that issued the advance to the paying agent is authorized to conduct unannounced cash verifications and may also require a specific format for reporting internal monthly verifications. The following is not to interfere with these unique requirements.

b. Verification of the paying agent's advance is similar to that for revolving advance holders. These guidelines add to those requirements.

(1) The paying agent's checking account will be reconciled to the most recent bank statement received. The current checking account balance will be determined. Outstanding checks will be reviewed for age. Checks over 30 days old (based on the last bank statement date) should result in a query to the payee for status.

(2) The total value of every submitted DD Form 281, but not yet paid by the disbursing officer, will be determined.

(3) Add the checking account balance and any outstanding DD Form 281 to the other assets and compare the total to the paying agent's authorized advance.

c. Resolving Discrepancies

(1) Discrepancies will be fully investigated and documented. In the event that a discrepancy cannot be resolved, a full report will be prepared and forwarded to the field office for review and appropriate action. If the discrepancy is such that a willful breach of fiduciary responsibility is indicated, then the individual will be relieved immediately of all responsibility for EEE funds and a new advance holder will be appointed. Strict accountability of the advance will be adhered to until a full investigation has been completed with a resolution reached. If after 24 hours the discrepancies are still unresolved, the situation will be reported to the applicable paying agent, SAC, Comptroller and IG.

(2) Reference (f) contains detailed guidance and procedures on dealing with missing or lost funds. While the provisions thereof must be complied with on a full and complete basis, it is also necessary to ensure that NCISHQ is advised whenever such instances occur. Accordingly, copies of any and all documentation submitted via the local disbursing office pursuant to resolving the loss of funds, or requesting relief from liability will be forwarded to the Comptroller, with an informational copy to the IG.

37-16. Review of Expenditures

a. Upon receipt of a DD Form 281 with accompanying claims and sub-vouchers at NCISHQ, the Comptroller's office will examine all associated documentation to verify compliance with applicable guidance as established in this chapter and by appropriate authority. Discrepancies and deficiencies will be referred for clarification or correction to the parent field office submitting the claims.

b. The Comptroller may also refer random NCIS Form 030, with associated sub-vouchers, to the Criminal Investigations Directorate, National Security Directorate, Global Operations or geographic EAD as appropriate for reconciliation with case files and/or asset dossiers. In such cases, reports will be provided back to the Comptroller, which identify any discrepancies or improprieties.

c. A system for tracking all referrals will be maintained by the Comptroller for follow up purposes. Action on claims referred for correction or clarification must be reported back to that office within 30 days of receipt at the affected field office.

d. The Comptroller may refer deficient or questionable claims to the IG. In such cases, the IG will ensure timely resolution of discrepancies and provide reports to all offices concerned with the claim(s).

e. Subsequent to these reviews being performed, all EEE documents will be returned to the EEE fund accounting technician for accounting and retention purposes.

37-17. Records Retention

a. The retention of records relating to EEE funds, unless otherwise stipulated in this chapter or by appropriate authority, will be as follows:

b. Copies of DD Form 281 will be held by each paying agent for the current and three prior fiscal years (absent any discrepancies).

c. Copies of NCIS Form 030 with attachments will be held at each field office for the current and two prior fiscal years (absent discrepancies) and then destroyed. Other offices that prepare NCIS Form 030 must retain their copies, with attachments, for one full year.

d. Original NCIS Form 028 is returned to the holder of the advance upon liquidation. Fund custodians will retain copies of NCIS Form 028 for three years (absent discrepancies).

e. Claims and associated documentation submitted to NCISHQ by field components will be retained by the Accounting Officer for six full fiscal years.

f. Copies of cash verification certifications will be retained until the next inspection conducted by the IG.

37-18. Correction and Collection of Erroneous and Improper Fee Expenses

a. Determination of Error or Impropriety. During the authorization, review, and audit phases of EEE fund administration, deficient claims are occasionally detected. Depending on the nature of the identified deficiency, corrective action may be required.

b. Erroneous Expenditures

(1) Erroneous expenditures are those which are chargeable to the EEE subhead but are either (1) deficient in the information provided on the associated claim forms, (2) charged to an improper expense category, or (3) otherwise erroneous with regard to documentation or processing. Erroneous claims will be corrected as follows: If the claim has not yet been reported and expended in the official accounting records (i.e., claimed on DD Form 281 by a paying agent), then the individual who first detects the error will refer the claim back down the administrative chain to the original claimant or otherwise appropriate office for correction. Appropriate training or counseling will be conducted to prevent a repeat of the error.

(2) Erroneous claims that are detected subsequent to entry in the official accounting records need only be corrected if they are charged to the wrong subhead (LE, CI or FOG). Upon discovering the requirement for corrective action the field office fund custodian should immediately notify the paying agent, who will notify the NCISHQ Accounting Officer. The accounting officer will initiate the appropriate accounting adjustments. Notification of corrective action will be forwarded down the administrative chain to the original claimant. Associated documentation will be annotated to clearly reflect the nature of and reason for any corrective action taken. Should the nature of the error require resubmission of original documents (NCIS Form 029 or NCIS Form 030), then the Comptroller's office will forward a notification of requirements to the office or individual responsible for resubmission with appropriate notification of the paying agent.

c. Improper Expenditures

(1) Improper expenditures are those that are, at some point in the administrative process, determined to be not chargeable to the EEE subhead. This determination may be made by any of the officials normally involved in the EEE administrative chain, including personnel attached to non NCIS oversight agencies (i.e., Naval Audit Service). All improper expenditures and claims must be corrected, whether by collection or reclassification. The following subparagraphs detail procedures for effecting corrective action regarding improper expenditures.

(2) Expenditures which are determined to be not allowable under the EEE subhead, but are properly chargeable to another Navy subhead, will be corrected as follows:

(a) For improper expenses not yet claimed on DD Form 281 (entered into the official accounting records): If the expense is one which is properly reimbursable utilizing SF 1164, then the claim will be referred to the original claimant for resubmission on that form. The claimant will reimburse the EEE fund custodian for the amount of the erroneous claim.

(b) If the claim has been expended against the EEE subhead and entered into the official accounting records (i.e., a DD Form 281 has been submitted), then corrective action must be

taken by the NCISHQ accounting officer. Fund custodians will maintain a log of all claims referred for corrective action for follow-up purposes. It is the responsibility of the field office fund custodian to ensure all required action is completed. Instances of non-cooperation or non-compliance will be referred to the senior supervisory official at the field office (or, NCISHQ) for action.

d. Expenditures that are not properly chargeable to any Navy appropriation, or, subhead thereof, will be disallowed. If a claim is paid and charged to the EEE subhead and is subsequently determined to be not chargeable to any Navy appropriation, then the individual(s) submitting and/or authorizing the original claim will assume personal liability for the expense. Reimbursement will be obtained as soon as possible (normally within 72 hours of identification and determination of the impropriety), utilizing the individual's personal funds.

e. Paying agent will execute collection documents, including those necessary to correct the official accounting records. Any person accepting funds on behalf of NCIS pertaining to a disallowed EEE claim will provide a receipt to the person on whom liability exists. The collected funds will be forwarded to the appropriate paying agent along with an explanation of the correction to include from whom and why funds were collected.

f. In cases where criminal impropriety appears to exist, the senior NCIS official (SAC level) will be notified, who in turn will initiate such action as is prudent and called for under existing law or regulations. In all such instances, the NCIS IG will be notified.

g. Repetitive instances of improper claims by an office or individual will be researched for cause and, if necessary, corrective measures will be initiated which provide reasonable assurance that a future violation will not occur.

h. Requests for relief of personal liability, when such is indicated, will be submitted in accordance with reference (f), as amended periodically. Copies of all correspondence and endorsements received from/submitted to local disbursing offices will be forwarded to the NCIS IG for informational purposes.

i. Reporting Corrective Actions Taken

(1) All corrective actions taken as a result of the identification of deficiencies and which result in changes to previously reported obligations shall be reported to the NCIS Comptroller's office via debits and credits to the monthly report of obligations. Paragraph 5 of that report will be annotated to reflect the nature of any significant corrections.

(2) All other initiatives taken in regard to the correction of procedures, management actions, disciplinary actions, or investigations of impropriety, as they relate to EEE fund administration will be reported to the NCIS IG via e-mail or Gen Admin. The IG may elect, in turn, to further comment or request additional action with regards to the reported initiative(s).

Appendix A: Bulk Memento Log

BULK MEMENTO LOG

ITEM:

DATE	QUANTITY		DETAILS (FROM/TO)	BALANCE ON HAND
	IN	OUT		

Appendix B: Appointment as Paying Agent

Use the DD 577, Appointment/Termination Record – Authorized Signature. The form is available on the Internet. Fill in as follows:

1. NAME	Insert Comptroller's Name
2. TITLE	Comptroller
3. DOD COMPONENT	DON/Naval Criminal Investigative Service
4. DATE	
5. SIGNATURE	
6. NAME	
7. SSN	
8. TITLE	Paying Agent
9. DOD COMPONENT	DON/Naval Criminal Investigative Service
10. ADDRESS	Field Office/Department
11. TELEPHONE	
12. EFFECTIVE DATE	
13. POSITION	Other: Paying Agent

14. "You are hereby appointed as Paying Agent representing {indicate Disbursing Office where advance is obtained} from whom your advance was obtained and to whom you are accountable. Your duties include accounting for cash and other assets in accordance with the below references. The maximum advance that you may hold under this appointment is ${copy amount from prior Agent's DD577, or contact the Comptroller if a change is desired}. Your actual advance should be the minimum necessary to perform your duties.

You shall be responsible for the advance issued to you. The purpose of this advance is for the administration of the organization's Emergency and Extraordinary Expense Funds (EEE). This appointment shall continue in force until you are transferred or relieved of duty by the appointing official."

15. DODFMR, Volume 5, Chapter 02
DODFMR, Volume 5, Chapter 03
Manual for Administrative, NCIS-1, Chapter 37

16. PRINTED NAME

17. SIGNATURE

Appendix C: Appointment as Fund Custodian

Use the DD 577, Appointment/Termination Record – Authorized Signature. The form is available on the internet. Fill in as follows:

1. NAME	SAC/DAD Name
2. TITLE	SAC/DAD
3. DOD COMPONENT	DON/Naval Criminal Investigative Service
4. DATE	
5. SIGNATURE	SAC/DAD
6. NAME	
7. SSN	
8. TITLE	Fund Custodian
9. DOD COMPONENT	DON/Naval Criminal Investigative Service
10. ADDRESS	Field Office/Department
11. TELEPHONE	
12. EFFECTIVE DATE	
13. POSITION	Other: Fund Custodian

14. "You are hereby appointed as Fund Custodian servicing the Naval Criminal Investigative Service, {indicate office/Department}. This appointment shall continue in force until you are transferred or relieved of duty by the appointing official.

You shall be responsible for the advance issued to you. The purpose of this advance, which will vary based on need, is for the administration of the organization's Emergency and Extraordinary Expense Funds (EEE) in accordance with the below references."

15. DODFMR, Volume 5, Chapter 02

DODFMR, Volume 5, Chapter 03

Manual for Administrative, NCIS-1, Chapter 37

16. PRINTED NAME

17. SIGNATURE

Appendix D: NCIS Form 028 - Request for Advance of EEE Funds

REQUEST FOR ADVANCE OF EEE FUNDS

The requestor agrees to be held personally liable for the amount provided and will comply with procedures detailed in NCIS 1, Chapter 37.

1. Requester	*2. Location*	*3. Phone*
4. Date	*5. Amount*	*6. Needed no later than*
7a. Type	*7b. Purpose*	
For One Time Advances, the requester acknowledges that all sub-vouchers and any excess funds will be turned in within five days of completion. Estimated Completion Date: _____		
8. Special Instructions		
9a. Requester Signature	*9b. Requester Title*	*9c. Date*
10a. Approver's Signature	*10b. Approver's Title*	*10c. Date*

Cash Receipt Certificate

11a. Received From (Custodian Name)	*11b. Custodian Signature*	
12. Amount		
13. Requester Signature	*14. Check Number (If Applicable)*	*15. Date*

Liquidation Information

Upon Liquidation, Requester receives (voided) original. Advancer retains (voided) copy.

16. Date Advance was Liquidated	*17. Requester Signature*
18. Method of Liquidation (Claim Number, Cash, Check # or Combination)	

NCIS FORM 028/9/03

Appendix E: Instructions for Sub-Voucher (Form 029)

EEE expenditures can be either Confidential or Unclassified. Sub-voucher forms are available for each type: 029c and 029u. Other than their classification markings, they are identical. No information classified higher than Confidential will be written on or attached to the Form 029c. No Confidential information will be written on or attached to the Form 029u. Specific, line-by-line instructions for completing this form are as follows:

1. SOURCE - When an asset or DA is utilized pursuant to the claim, then the source's NCIS number or code name will be annotated. This block will usually be completed for rewards and asset expenses. If none, insert the designation "N/A" (not applicable).

2. CCN - Complete the case control or intelligence/operation report number, if one is assigned. If none, insert the designation "N/A."

3. CASE OR OPERATION TITLE - Case/operation names, if designated. Use "N/A" when appropriate.

4. RECEIPTS - This block MUST BE COMPLETED. If original receipts are obtained, tape them to the lower half of the Form 29 or on a continuation sheet. If a TNR was obtained, indicate such. DO NOT FORWARD A TNR WITH THE FORM 029. If a TNR should have been obtained, but was not, provide full and complete explanation in Block 9 of this form. Consult NCIS-3, Chapter 8 for additional information on payments requiring a TNR. If original receipts were not obtained for all or any portion of the claim, then a full and complete explanation must be provided in block 9. Likewise, if the receipt is for an amount other than that claimed, provide an explanation. Supervisors should not approve sub-vouchers that are incomplete. Statements such as "NO RECEIPT OBTAINED" will not be accepted. The total amounts listed in this block may not be equal to that claimed in Block 12 if a TNR was obtained from a source, but the source also provided actual vendor receipts.

5. DATE(s) - Provide the date that the expenditure took place and when the sub-voucher is submitted for approval/reimbursement.

6. SUB-VOUCHER NO. - Leave blank. The fund custodian will fill in while constructing the claim submission.

7. GENERAL EXPENSE CATEGORY - This block is already completed, listing whether the form holds counterintelligence or law enforcement expenses. (Fleet Operations Group expenses shall always use the form 029c.)

8. SPECIFIC EXPENSE CATEGORY - Indicate the specific expense category applicable to this disbursement. Consult section 37-9 for guidance on which category is most appropriate. Check only one category.

9. REMARKS - this block should include a complete description of the nature of the expense. A clear justification for the need to expend EEE funds will be provided. Specific categories may require particular information in this block based on guidance provided in section 37-9. At a minimum, the information provided will clearly establish the propriety of the claim, the reason for the expense, the vendor or individual receiving the funds, and the disposition of any items purchased. Data should be specific, clear, and concise. Use of uncommon acronyms and abbreviations is discouraged unless otherwise authorized in this chapter. When authorization is

Appendix E (Continued)
Instructions for Sub-Voucher (Form 029)

required prior to incurring an expense, note who approved the expenditure and the date of approval. If additional information regarding this expense is maintained in source records or case files, it should be so noted here. Foreign currency conversion rates, when applicable to the expense, will also be annotated in this space.

10. REPORTING OFFICE – The four character alphanumeric designator of the office to which the claimant is assigned should be noted in this block. Personnel traveling in a TDY status to another location will insert the designator for the office which provided the advance or which is sponsoring the activity or expense being incurred. The sub-voucher will be submitted to the office designated in this block.

11. SUPERVISOR'S SIGNATURE- Claimant's on-site supervisor, authorizing reimbursement by fund custodian.

12. TOTAL EXPENDED - Insert the total amount being claimed.

13. SUBMITTER'S SIGNATURE – A signature confirms that the expense occurred and the submitter has been fully reimbursed for any personal funds used.

Appendix E – Enclosure (1)
NCIS Form 029c – Counterintelligence and FOG (Classified) Expenses

SUB-VOUCHER FOR DISBURSEMENT OF EEE FUNDS

CONFIDENTIAL (When filled in)

1. Source:	2. CCN:	3. Case or Operation Title:

4. Receipts:	5. Date Claim Submitted:	6. Sub-voucher No.:
Receipts attached for: $ True Name Receipt on file for: $ Receipts not obtained for: $	Date of event:	

7. Type of Claim:

☒ **Counterintelligence**

8. Type of Expenditure: (Check one)

- ☐ Liaison
- ☐ Bulk Mementos
- ☐ Operational
- ☐ Protective Operations
- ☐ Non-Consumed Equipment
- ☐ Undercover
- ☐ Rewards
- ☐ (b)(7)(E)
- ☐ Evidence Buy/Walk? ☐
  Buy/Bust? ☐ ($ Log#)
- ☐ Miscellaneous

9. Remarks:

Comments Needed for: Non-use of Regular Funding / Present or Future Value of Liaison Contact(s) / Advance Approval

TDY Status a Factor? ☐Yes (Show Calculations) ☐No

Conversion Rate: = $1.00 US (If Applicable)

10. Reporting Office:	11a. Concurring Supervisor:	11b: Supervisor's Signature:	11c. Date:
12. Total Expended:	13a. Submitted by:	13b. Submitter's Signature:	13c. Date:

INSTRUCTIONS:

1. Form must be typed.
2. Attach receipts here or on continuation sheets with tape. Do not staple.
3. Use "CONFIDENTIAL" safeguards for all completed forms.
4. Present to the fund custodian or paying agent for reimbursement.
5. Under normal circumstances, submit claims within five days of the expenditure.

CONFIDENTIAL
(When filled in)

NCIS FORM 029c/04/12

Appendix E – Enclosure (2)
NCIS Form 029c – Sample Sub-Voucher

SUB-VOUCHER FOR DISBURSEMENT OF EEE FUNDS

CONFIDENTIAL (When filled in)

1. Source:	2. CCN:	3. Case or Operation Title:
EUNA-0123	10OCT00-EUNA-0745-5ANA	TECH TRANSFER TO HOIS

4. Receipts:	5. Date Claim Submitted:	6. Sub-voucher No.:
Receipts attached for: $ True Name Receipt on file for: $ Receipts not obtained for: $ 400.00	01/13/12 Date of event: 01/12/12	

7. Type of Claim:

☒ **Counterintelligence**

8. Type of Expenditure: (Check one)

- ☐ Liaison
- ☐ Bulk Mementos
- ☒ Operational
- ☐ Protective Operations
- ☐ Non-Consumed Equipment
- ☐ Undercover
- ☐ Rewards
- ☐ (b)(7)(E)
- ☐ Evidence Buy/Walk? ☐ Buy/Bust? ☐ ($ Log#)
- ☐ Miscellaneous

9. Remarks:

Funds provided to source to cover expenses incurred (local travel, reward to sub-sources, meals, etc.) during performance of NCIS tasking in subject investigation. Most expenses incurred while accompanying suspects, which necessitated not obtaining receipts for expenses. Activity was conducted in area around Naval Base, Naples, while under observation of Case Agent.

SAMPLE ONLY

Comments Needed for: Non-use of Regular Funding / Present or Future Value of Liaison Contact(s) / Advance Approval

TDY Status a Factor? ☐Yes (Show Calculations) ☐No | Conversion Rate: = $1.00 US (If Applicable)

10. Reporting Office:	11a. Concurring Supervisor:	11b: Supervisor's Signature:	11c. Date:
EUNA	John A. Smith		
12. Total Expended:	**13a. Submitted by:**	**13b. Submitter's Signature:**	**13c. Date:**
400.00	SA M. Harmon		

INSTRUCTIONS:

1. Form must be typed.
2. Attach receipts here or on continuation sheets with tape. Do not staple.
3. Use "CONFIDENTIAL" safeguards for all completed forms.
4. Present to the fund custodian or paying agent for reimbursement.
5. Under normal circumstances, submit claims within five days of the expenditure.

CONFIDENTIAL
(When filled in)

NCIS FORM 029c/04/12

Appendix E – Enclosure (3)
NCIS Form 029u – Sub-Voucher for Law Enforcement (Unclassified) Expenses

SUB-VOUCHER FOR DISBURSEMENT OF EEE FUNDS

For Official Use Only

1. Source:	2. CCN:	3. Case or Operation Title:

4. Receipts:	5. Date Claim Submitted:	6. Sub-voucher No.:
Receipts attached for: $ True Name Receipt on file for: $ Receipts not obtained for: $	Date of event:	

7. Type of Claim:

☒ **Law Enforcement**

8. Type of Expenditure: (Check one)

- ☐ Liaison
- ☐ Bulk Mementos
- ☐ Operational
- ☐ Protective Operations
- ☐ Non-Consumed Equipment
- ☐ Undercover
- ☐ Rewards
- ☐ (b)(7)(E)
- ☐ Evidence Buy/Walk? ☐ Buy/Bust? ☐ ($ Log#)
- ☐ Miscellaneous

9. Remarks:

Comments Needed for: Non-use of Regular Funding / Present or Future Value of Liaison Contact(s) / Advance Approval

TDY Status a Factor? ☐Yes (Show Calculations) ☐No Conversion Rate: = $1.00 US (If Applicable)

10. Reporting Office:	11a. Concurring Supervisor:	11b: Supervisor's Signature:	11c. Date:
12. Total Expended:	13a. Submitted by:	13b. Submitter's Signature:	13c. Date:

INSTRUCTIONS:
1. Form must be typed.
2. Attach receipts here or on continuation sheets with tape. Do not staple.
3. Provided no classified information!
4. Present to the fund custodian or paying agent for reimbursement.
5. Under normal circumstances, submit claims within five days of the expenditure.

For Official Use Only

NCIS FORM 029u/04/12

Appendix E – Enclosure (4)
NCIS Form 029u – Sample Sub-Voucher

SUB-VOUCHER FOR DISBURSEMENT OF EEE FUNDS

For Official Use Only

1. Source:	2. CCN:	3. Case or Operation Title:

4. Receipts:	5. Date Claim Submitted: 12/23/11	6. Sub-voucher No.:
Receipts attached for: $ 432.50		
True Name Receipt on file for: $ 60.00		
Receipts not obtained for: $	Date of event: 12/22/11	

7. Type of Claim:

☒ **Law Enforcement**

8. Type of Expenditure: (Check one)

- ☒ Liaison
- ☐ Bulk Mementos
- ☐ Operational
- ☐ Protective Operations
- ☐ Non-Consumed Equipment
- ☐ Undercover
- ☐ Rewards
- ☐ (b)(7)(E)
- ☐ Evidence Buy/Walk? ☐ Buy/Bust? ☐ ($ Log#)
- ☐ Miscellaneous

9. Remarks:

Funds paid to "DC EVENTS" for catering fees, food, beverages, set-ups for bar drinks and tips for two workers and one bartender; held at Riverview Room, NAS Anacostia, for DCWA annual Christmas party. Guest list and list of NCIS personnel attending is attached. All attendees have provided and are expected to continue to provide assistance to DCWA. Receipt for tips to workers and bartender was not obtained. All others are attached. This expense was authorized by 0001 during telephone conversation w/SAC, DCWA on 28NOV00.

SAMPLE ONLY

Comments Needed for: Non-use of Regular Funding / Present or Future Value of Liaison Contact(s) / Advance Approval

TDY Status a Factor? ☐ Yes (Show Calculations) ☒ No | Conversion Rate: = $1.00 US (If Applicable)

10. Reporting Office:	11a. Concurring Supervisor:	11b: Supervisor's Signature:	11c. Date:
DCWA	K SISCO		
12. Total Expended:	**13a. Submitted by:**	**13b. Submitter's Signature:**	**13c. Date:**
492.50	M. HARMON		

INSTRUCTIONS:
1. Form must be typed.
2. Attach receipts here or on continuation sheets with tape. Do not staple.
3. Provided no classified information!
4. Present to the fund custodian or paying agent for reimbursement.
5. Under normal circumstances, submit claims within five days of the expenditure.

For Official Use Only

NCIS FORM 029u/04/12

Appendix F: Instructions for Claim (Form 030)

a. Fund custodians and personnel assigned responsibility for special events requiring the use of EEE funds (i.e. convention coordinators, detail leaders for protective operations) will prepare this form. Responsibility for complete and accurate information is vested in these persons. It will be filed not less than monthly for the purpose of replenishing office EEE advances and for reporting the expenditure of EEE funds. If an office has no occasion to submit a claim for the month, appropriate notification will be made to the field office fund custodian and in turn to the designated paying agent.

b. The original form with accompanying original sub-vouchers will be forwarded to the parent fund custodian. This fund custodian will consolidate all Forms 030 received from subordinate fund custodians and submit them to the designated paying agent for reimbursement. Consolidated Forms 030 (less the supporting Form 029) and a copy of the most recently completed audit/cash verification of funds will be faxed to paying agent, with the complete package forwarded via mail.

c. The paying agent will, upon receipt of the faxed documentation, process claims for reimbursement and issue checks to the funds custodians who prepared each Form 030. The paying agent will utilize the information and documentation provided for the purpose of tracking EEE funds and for completing the "Voucher for Confidential Expenditures" (DD Form 281).

d. Two versions of the Form 030 are available. Form 030u is for submission with unclassified sub-vouchers. Form 030c is for classified sub-vouchers. (FOG related expenses will be consolidated on separate claims, clearly marked as FOG.)

e. All completed Forms 030, when appended with completed sub-vouchers, will be classified at the same level as the attached sub-vouchers. Even though the "CONFIDENTIAL" designation is preprinted on the form, filers are strongly encouraged to prominently stamp the designation in red ink on the top and bottom of completed forms.

f. Specific line by line instructions for completing this form are as:

CLAIM # - Insert the four-character code for the office filing claim, last two digits of fiscal year and three-digit serialized number. Each fund custodian will assign serial numbers in the format XXXXFY-001.

OFFICE - Insert the four-character office code for each office filing the claim (i.e., DCWA, NCIS 23).

PREPARED BY – The preparer will print their name, sign where indicated, and insert the date the claim is actually presented for payment/reimbursement.

FROM - Insert the date of the oldest sub-voucher accompanying the claim.

TO - Insert the date of the most recent sub-voucher accompanying the claim.

CONCURRENCE – Two levels of supervisory concurrence above the preparer may be used.

NOTE: Personnel signing as concurring/approving officials must not have submitted Form 29's that are attached to subject claim.

Appendix F (Continued)
Instructions for Claim (Form 030)

FIRST LEVEL -The immediate supervisor of the preparer. In the event there is no intervening supervisor between the preparer of the claim and the official authorized as the second level concurrence, the First Level should be crossed out.

SECOND LEVEL – An ASAC for the field office, and DAD for NCISHQ.

APPROVAL - Field office SAC, Department or Directorate Head.

AMOUNT PAID/ON/CHECK # OR RECIPIENT'S SIGNATURE - Completed by the paying agent at time of reimbursement. Most reimbursements will be made by check. On those occasions when a cash reimbursement is made, the recipient will sign in the appropriate space.

SUB-VOUCHERS INCLUDED - List each sub-voucher accompanying the claim; the type of General Expense Category (i.e., LE or FCI); the Specific Expense Category (i.e., Liaison or Cooperating Witness); the amount of the expenditure. SEPARATE CLAIMS (FORM 030) WILL BE SUBMITTED FOR EACH TYPE/GENERAL EXPENSE CATEGORY (LE OR FCI) AND SPECIFICALLY DESIGNATED SPECIAL OPERATIONS. Sub-voucher numbers, assigned by the preparer, will indicate the first two digits as the fiscal year followed by a three-digit serial number (i.e., 00-001, 00-002, 00-003).

EXPENSES BY CATEGORY (TOTALS) - Provide the total dollar value of sub-vouchers attached by each specific expense category.

TOTALS (BY LE OR FCI) - Total the amounts listed for law enforcement (LE) and counterintelligence (FCI).

CLAIM TOTAL - This figure should equal the total of all sub-vouchers listed and be the same total listed for Expenses by Category.

Attach all Form 029s and supporting documents.

Appendix F – Enclosure (1)
NCIS Form 030c – Claim for Counterintelligence and FOG (Classified) Expenses

COUNTERINTELLIGENCE

CLAIM FOR CONFIDENTIAL EXPENSES

CONFIDENTIAL
(With Enclosures Attached)

Claim #

Office _____ Prepared by _____ _____
From To Signature Date

Concurrence

1st Level Position

_____ _____ _____ _____
Signature Date

2nd Level Position

_____ _____ _____ _____
Signature Date

Approval Position

_____ _____ _____ _____
Signature Date

Amount Paid: $ _____ On: _____ Check # or

Recipient's Signature: _____

Sub-vouchers Included

SV#	Category	Amount
Total		

Expenses by Category

Category	Amount (FCI ONLY)
Liaison	
Bulk Mementos	
Operational	
Protective Operations	
Non-Consumed Equipment	
Undercover Expenses	
Rewards	
(b)(7)(E)	
Evidence	
Miscellaneous	
Total	

Claim # _____

Appendix F – Enclosure (2)
NCIS Form 030u – Claim for Law Enforcement Expenses

LAW ENFORCEMENT
CLAIM FOR EXPENSES **FOR OFFICIAL USE ONLY**

Claim #

Office Prepared by

From To Signature Date

Concurrence

1st Level Position

Signature Date

2nd Level Position

Signature Date

Approval Position

Signature Date

Amount Paid: $ _____ On: _____ Check # or

Recipient's Signature: _____

Sub-vouchers Included

SV#	Category	Amount
Total		

Expenses by Category

Category	Amount (LE ONLY)
Liaison	
Bulk Mementos	
Operational	
Protective Operations	
Non-Consumed Equipment	
Undercover Expenses	
Rewards	
(b)(7)(E)	
Evidence	
Miscellaneous	
Total	

Claim # _____

FOR OFFICIAL USE ONLY

Appendix G: EEE Verification Worksheet

EEE Verification Worksheet

1. Cash on Hand				3. Sub-vouchers on Hand (Form 029s)	
1a. Coins	Quantity	Value		Sub-voucher #	Amount
$1.00					
$0.50					
$0.25					
$0.10					
$0.05					
$0.01					
		Total Coins			
1b. Currency	Quantity	Value			
$100					
$50					
$20					
$10					
$5					
$1					
		Total Currency		Total Sub-vouchers	
		Reimbursement Checks Not Cashed		4. Outstanding Claims	
		Total Cash on Hand		Claim #	Amount

2. Advances Out				
Name	Date Due Back	Amount		
			Total Claims	
			5. Checking Account (Agent Cashier Only)	
			Current Balance	
			Verified (Initials)	
			6. DD281 (Agent Cashier Only)	
			Amount	
		Total Advances	Verified (Initials)	

Recapitulation	
1. Cash on Hand	
2. Advances	
3. Sub-vouchers	
4. Claims	
5. Checking Account	
6. DD-281s	
Total	

Advance Amount: _____ Form 28 Sighted (Initials) _____

Advance Holder: _____ Initials _____

Verified By: _____Title: _____

Signature: _____ Date: _____

NCIS FORM 027/04/12

CHAPTER 38
PERMANENT CHANGE OF STATION (PCS)
POC: CODE 10A
DATE: DEC 06

POLICY DOCUMENT

APPENDIX (F) Gen Admin 11C-0041 of 02Dec11 released NCIS Policy Document No. 11-24 Administrative (Rental Property Management Program). Policy document 11-24 contains revised or new policy that has not been incorporated into this chapter and should be reviewed in its entirety.

APPENDIX (G) Gen Admin 11C-0003 of 11 Jan 16 released NCIS Policy Document No.16-01 Administrative (PCS Travel). Policy document 16-01 contains revised or new policy that has not been incorporated into this chapter and should be reviewed in its entirety.

38-1. PURPOSE

This chapter identifies the procedures, entitlements and allowances associated with a Permanent Change of Station (PCS) within CONUS, to/from an overseas post, or to/from a foreign area for employees of the Naval Criminal Investigative Service (NCIS). This guide supplements but does not replace or take precedence over the Joint Travel Regulations (JTR), Volume 11.

38-2. BACKGROUND

The Department of Defense (DoD) issues policy on PCS travel for civilians in the Joint Travel Regulations (JTR), Vol II. The Department of State (DOS) issues policy, guidance, and updates for entitlements and allowances in foreign areas in the Standardized Overseas Regulations (SOR). This chapter supplements these policies by answering some of the frequently asked questions concerning PCS travel specifically for NCIS employees.

38-3. DEFINITIONS

a. Permanent Change of Station (PCS). The official transfer of an employee from one permanent duty station to another.

b. Official Travel Orders. The document detailing the specific entitlements and allowances applicable to the employee executing a PCS.

c. Dependent. Any of the following named members of the employee's household at the time the employee reports for duty at the permanent duty station or performs authorized/approved renewal agreement or separation travel:

(1) Employee's spouse; and/or,

(2) Children of the employee or the employee's spouse who are unmarried and under 21 years of age or who, regardless of age, are physically or mentally incapable of self-support. (The term "children" includes natural offspring; stepchildren; adopted children; grandchildren; legal minor wards, or other dependent children who are under legal guardianship of the employee or the employee's spouse; also, a child born after the employee's effective date of transfer and then moved when delay in move is caused by the mother's advance stage of pregnancy, or other reasons acceptable to the DoD component concerned, e.g., awaiting completion of the school year by other children.); and/or,

(3) Dependent parents (including step- and legally adoptive parents) of the employee or the employee's spouse; and/or,

(4) Dependent brothers and sisters (including step- and legally adopted brothers and sisters) of the employee or the employee's spouse who are unmarried and under 21 years of age or who, regardless of age, are physically or mentally incapable of self-support.

d. Temporary Quarters Subsistence Expense (TQSE) - An allowance that compensates the employee for certain expenses incurred while seeking/awaiting a permanent residence at the new duty station in the United States, its territories or possessions.

e. Temporary Quarters Subsistence Allowance (TQSA) - An allowance that compensates an employee for certain expenses incurred at the beginning and end of a tour of duty in a foreign area while seeking/awaiting permanent quarters or awaiting household goods (HHG). At the end of the tour, this allowance is intended to permit early HHG shipment to the new duty station and thereby reduce the requirement for temporary quarters at the new duty station.

f. Living Quarters Allowance (LQA) - Essentially, a housing subsidy at the assigned duty station. It pertains only at certain overseas posts and pertinent guidance is set forth in the DOS Standardized Overseas Regulations.

g. Foreign Transfer Allowance (FTA) - An allowance that compensates an employee for subsistence expenses incurred before final departure from a duty station in the 50 states and Washington, D.C., to a duty station in a foreign area.

h. United States - For PCS purposes, the 50 states, the District of Columbia, and U.S. territories and possessions.

i. CONUS - For PCS purposes, the 48 contiguous states and the District of Columbia.

j. Foreign Area – Any area or country outside the 50 states and the District of Columbia, the Commonwealths of Puerto Rico and the Northern Mariana Islands, Guam and U.S. territories and possessions.

k. Overseas - For PCS purposes, any non-Foreign area outside CONUS.

l. AMC, Category M - The Air Mobility Command (AMC) transportation with military passenger configured aircraft used to transport passengers. This type of transportation is billed to the Navy at the U.S. Government rate tariff and requires an AMC Transportation Authorization.

m. AMC, Category Y – AMC-contracted blocks of seats on regularly scheduled commercial flights. This type of transportation is billed to the Navy at the U.S. Government rate tariff and requires an AMC Transportation Authorization.

n. Category Z (CATZ) - Travel on regularly scheduled U.S. flag international air carriers with tickets procured directly from the air carrier with Government Transportation Requests (GTR).

38-4. STANDARD ALLOWANCES

a. CONUS to CONUS PCS - Concurrent transportation of dependents, if desired; POV or commercial air travel to the new duty station; Government Bill of Lading (GBL) (SF 1103) shipment of HHG; per diem for employee and dependents; house-hunting trip (if requested and approved); TQSE (if required); miscellaneous expense allowance; real estate benefits; temporary storage of HHG.

b. CONUS to OVERSEAS (Non-Foreign Area) - Concurrent transportation of dependents (in most cases); POV mileage to designated POV shipping terminal and return; air transportation to new duty station; per diem for employee and dependents; TQSE (if required); miscellaneous expense allowance; real estate benefits; GBL shipment of HHG; non-temporary storage of HHG; temporary storage of HHG; shipment of POV.

c. CONUS to FOREIGN AREA - Concurrent transportation of dependents (in most cases); POV mileage to designated POV shipping terminal and return; air transportation to new duty station; per diem for employee and dependents; FTA in CONUS and TQSA after arrival at new duty station: miscellaneous expense allowance; GBL shipment of HHG; non-temporary storage of HHG; temporary storage of HHG; shipment of POV.

d. OVERSEAS (Non-Foreign Area) to CONUS - Concurrent transportation of dependents (in most cases); air transportation to new duty station or POV shipping terminal in CONUS and

POV mileage from shipping terminal to new duty station; per diem for employee and dependents; TQSE (if required); miscellaneous expense allowance; real estate benefits; GBL shipment of HHG; temporary storage of HHG; shipment of POV (provided a POV was shipped from CONUS to overseas).

e. FOREIGN AREA to CONUS - Concurrent transportation of dependents (in most cases); air transportation to new duty station or air transportation to POV shipping terminal in CONUS and POV mileage to new duty station; per diem for employee and dependents; TQSA in foreign area prior to departure and TQSE after arrival in CONUS (if required); miscellaneous expense allowance; shipment of POV (provided a POV was shipped from CONUS to the foreign area); real estate expenses (provided transfer is to a different official station in CONUS than the one from which the employee transferred when assigned to the foreign post of duty).

38-5. THE NCIS PCS PROGRAM

a. Notification

(1) Typically, a General Administration (Gen Admin) document is issued and transmitted to officially notify the employee of his/her selection for assignment to a new duty station. To the extent information is available at time of notification, the Gen Admin will identify the new duty station and the approximate reporting date. It will direct the employee to complete and submit a travel questionnaire.

(2) As appropriate, the Gen Admin will also advise the employee to obtain or update official passports and all necessary inoculations. A PCS Planning Checklist (appendix A) is provided to use as a guide during the PCS process.

(3) To ensure that all possible entitlements and allowances are included in the orders, employees should pay careful attention to the following items on the travel questionnaire:

(a) Complete identifying information on all eligible dependents and a statement of whether concurrent travel of dependents is preferred.

(b) A well-defined itinerary, including a statement concerning the use of annual leave enroute. It should be noted that leave enroute must be coordinated between the losing and gaining offices. NCISHQ does not authorize leave for field personnel unless NCISHQ is the gaining office.

(c) Full details regarding any unique situations or problems. Many such situations can be resolved before a PCS actually begins; considerable difficulty can result from after-the-fact attempts to handle a problem.

b. Transportation Agreement

(1) Before cost PCS orders are issued, the employee must complete and sign a transportation agreement. Transportation agreements stipulate that the employee remain in

Government service for at least 12 months beginning with the date he/she reports for duty at the new duty station (unless separated for reasons beyond the employee's control and/or for reasons acceptable to NCISHQ, Code 10. Failure to fulfill the terms of this agreement may result in indebtedness to the Government for any travel and transportation costs extended by the Government relative to the PCS move. The original transportation agreement will be filed in the employee's Official Personnel Folder. A signed copy of the transportation agreement will be forwarded to Code 10A to initiate preparation of travel orders.

(2) When the new duty station is located in CONUS, the employee will be required to complete and sign FORM DD-1618, DoD Transportation Agreement-Transfer of Civilian Employees To and Within Continental United States.

(3) For transfers to overseas areas, the employee will be required to complete and sign FORM DD-1617, Transportation Agreement-Overseas Employee. In addition to the 12-months service requirement detailed above, the DD-1617 will reflect the prescribed overseas tour length. Until completion of the prescribed overseas tour, the employee will not be eligible for return travel at Government expense to his/her place of actual residence, unless the reason for earlier return is beyond the employee's control and acceptable to NCISHQ, Code 10.

(4) If an employee is assigned from one overseas duty station to another before completion of the prescribed tour length, the tour length at the new duty station will apply with credit given for prior service at the previous duty station. A new agreement is required with the new tour of duty being 12 months or the difference between the tour of duty at the new duty station and the period of service completed at the old duty station, whichever is greater.

(5) The DD-1617 contains a block to indicate the employee's place of actual residence or Home of Record. The Home of Record is not necessarily the location from which the employee is transferred overseas. Other factors may impact on the determination of the Home of Record. Such factors include home ownership, previous residency, temporary employment in the city from which recruited, employment requiring residence apart from the family, the employee's voting residence, and the place where the employee pays taxes. As renewal agreement travel and separation travel are limited to or from an employee's Home of Record, employees should ensure that the DD-1617 is completed accurately.

c. Travel Orders

(1) Once the travel questionnaire and appropriate transportation agreement have been received by NCISHQ Code 10A, official travel orders DD Form 1614 will be prepared. A copy of the orders will be faxed to the employee's current office. The original orders will be mailed to that office.

(2) Amendments.

(a) Changes in an employee's circumstances may necessitate an amendment to travel orders. Amendments are formal changes to existing orders made by endorsement. In most cases, an employee will not be paid for an expense if there is no written authorization for the

expense. If an unforeseen event occurs affecting the execution of the travel orders, the employee should check with Code 10A to ensure modification of orders is authorized and to seek adjustment of the travel cost estimate, if appropriate.

(b) Normally, the employee will be aware of the need for an amendment and should request one using a Gen Admin addressed to Code 10A. There will be cases when the need for an amendment is not identified until the claim is actually submitted. If at all possible, such requests will be acted upon immediately by Code 10A. However logical or reasonable a request may seem, if the change is not authorized in the JTR (Vol II), the change/modification cannot be granted.

Example: In executing PCS orders, the employee indicates he/she and dependents will travel by POV from the East Coast to the West Coast. An estimate will be made of the number of days required, based on the mileage involved. The travel orders may allow up to 7 days of transit per diem for which an advance of funds may be drawn. If the employee decides at the last moment to sell the family car and, with dependents, fly to the West Coast, the employee's per diem entitlement may be limited to three-fourths (3/4) of one (1) day.

(c) Amendments and authorizations can be made to travel orders at virtually any point in the process, within reason. The two principal determinants to amendments are whether they are permitted by JTR, VOL II, and whether the amendment requested is in the best interest of the government.

d. NCIS Sponsor System

(1) An employee at the new duty station will be designated to serve as a sponsor for the transferring employee. Both parties have responsibilities and effective communication must be established between the two parties early in the process. The designated sponsor must endeavor to make the transferring employee's PCS move as free from difficulty and confusion as possible. The sponsor must understand the relocating employee's requirements to help in a smooth transition to the new duty station. Likewise, the transferring employee must clearly express her/his requirements and interests to the sponsor.

(2) At a minimum, the prospective immediate supervisor will initiate contact with the transferring/newly-hired employee. This initial contact should be in writing, by e-mail, and should contain a welcome aboard greeting, some preliminary information regarding the office and community, and the assignment of a sponsor. Sponsors should be carefully chosen, e.g., special agents with children should have a special agent with children as a sponsor. It is then incumbent upon the transferring employee to acknowledge the first communication and identify the type and amount of information and/or assistance desired.

(3) Sponsors should be prepared to provide hard copy and/or electronic "links" to information via the internet to inbound transferring personnel. The attached checklist will serve as a guide to both the transferring and sponsor employees of types of information that may be of interest to the transferring employee. Transferring employees who require additional information must effectively communicate this to their sponsor. Sponsorship support should also

include assisting the transferring employee with obtaining the necessary access badges/parking placards upon arrival at the new duty station. Effective sponsorship at the workplace shall also include familiarization of the transferring employee with local administrative procedures, duty responsibilities (if applicable), and area familiarization

(4) Effective performance of sponsorship duties will be an area of interest reviewed during inpections conducted by NCISHQ Code 00I.

e. Using Duty Hours For PCS Related Matters

(1) A PCS move requires the relocating employee to perform certain key actions, which are properly a part of his/her official duties and not of a personal nature (e.g., real estate actions, activation/deactivation of utilities, license and vehicle registration, etc.) Accordingly, it is NCIS policy that a "reasonable" amount of duty time will be allowed a transferring employee to complete PCS-related actions.

(2) To achieve uniformity, NCIS supervisors and managers will, upon request of a transferring employee, allocate duty hours to the employee for specific non-personal PCS-related actions. Periods of absence are to be charged to administrative leave (ADLV) in the timekeeping system. The administrative leave may be used at the old or new permanent duty station or both, provided the appropriate absence does not exceed an aggregate of 40 hours.

38-6. KEEPING PRECISE TRAVEL RECORDS

a. It is important for all travelers to keep a record of expenses incurred while on official travel. A small pocket notebook is sufficient to record needed data. The following items should be tracked:

Date and hour of departure
Date and hour of arrival/departure at each stopping point
Mileage of POV at departure and at each stopping point
Cost of taxi fare
Meal expenses (including tips), by meal
Laundry expenses
Official telephone call costs
Lodging costs (obtain and retain receipts for anything over $25.00)
ALL expenses incident to vacating one residence and subsequent set up at the new duty station (e.g., disconnecting appliances, hanging drapes, cutting rugs, etc.)

b. The list of expenses can be substantial and varies with each travel incident. In every case, it is better to record and retain more details than not enough. Completion of travel claims is simplified with complete and detailed expense records and it is less likely that certain expenses will be overlooked when preparing the travel voucher.

c. The adequacy of expense records is particularly important when traveling to ”high cost" Per Diem areas. TQSE computations are based on the standard rate of per diem, NOT the high cost per diem, despite the fact the employee occupied temporary quarters in a high cost area. Miscalculation on this point can be very costly to the PCS traveler.

d. It is generally good practice to maintain a personal file for travel performed for a period of 3-years from the date of the settled claim. Such records should consist of the original travel orders, copies of the paid claim(s), and supporting documentation. Such records are invaluable in the event a claim is contested or required in conjunction with an IRS audit.

38-7. TRAVEL EXPENSES

a. Estimating Travel Expenses

(1) Travel orders provide a variety of authorizations for an employee and/or dependents performing official travel. During the travel order preparation process, an estimate is made of the funding required for authorized expenses. The estimate is based on advance information provided by the traveler through the travel questionnaire. The questionnaire is used to compute entitlements for per diem allowances, Privately Owned Vehicle (POV) mileage allowances, Temporary Quarters Subsistence (TQS) allowances, concurrent/non-concurrent travel of dependents, and air travel authorization. The questionnaire should be completed with as much care and forethought as possible. All desired adjustments for personal plans should be included, e.g., mode of transportation desired, detailed information on family member travel, planned departure and arrival dates, etc.

(2) Failure to provide complete and specific information in the questionnaire may result in the employee paying heavily out of pocket for PCS related expenses which might otherwise have been offset by an advance of funds.

(3) The questionnaire is also used to estimate expenses for real estate transactions, and the costs incurred in the shipment of HHG and POV if such items are shipped via GBL. Certain of these expenses are not compensable unless authorized in writing on the travel orders.

(4) PCS orders written for transfers to duty stations in a foreign country will contain no estimates of costs for Temporary Lodging Allowance (TLA). TLA is locally administered and paid at the new, overseas locations.

(5) Special Requirements. Reimbursement for travel expenses will be made in compliance with the JTR. The JTR imposes considerable responsibility on activities to have adequate justification for any obligations allowed. Requests for changes in allowances or other modifications of orders must be submitted in writing to NCISHQ Code 10A.

b. Advances

(1) An advance of funds will be authorized for certain expenses included on the PCS orders, i.e., per diem for enroute travel, POV travel, per diem for a HHT, TQSE and FTA. No

advance funds will be provided for other expenses on the PCS orders, e.g., air travel, miscellaneous expenses, shipment and storage of HHG and shipment of POV. The orders will specify the maximum amount of the advance. Employees are cautioned that most travel advances are paid as a direct deposit to the employee's bank account. As a result, the PCS orders may not reflect a Disbursing Office Voucher (DOV) stamp.

(2) Employees are reminded to accurately annotate their PCS claims with the amount of the advance paid so as to avoid a potential indebtedness situation at a later point. Keep in mind that this amount is only an estimate. The actual amount you will be reimbursed may be significantly higher or lower than the total authorized. Keep meticulous records of all your PCS-related expenses. This will help settle your claim and assist in preparing the following year's federal income tax return.

c. Foreign Area Advances

(1) The Foreign Service Act of 1980 authorizes a one-time advance of pay to civilian employees ordered to foreign areas on a permanent assignment. This entitlement does not apply when an individual is transferred from a foreign area.

(2) The advance pay may be requested by the employee 3 weeks prior to departure or no later than 3 months after arrival at the foreign duty station.

(3) The maximum amount to be advanced is three months' basic pay.

(4) Repayment will be made by means of payroll deduction over a period of up to 26 pay periods commencing with first pay period after receipt of the advance.

(5) Employee must agree to immediate lump-sum repayment of outstanding balance if employment is terminated prior to liquidation of advance.

(6) A request and voucher for advance of civilian pay (FORM SF-1190) will be provided at the time PCS orders to a foreign area are issued. FORM SF-1190 must be returned to NCISHQ Code 10A for processing through DFAS.

(7) Code 10A will obtain the necessary fund citation from Code 14 for the advance of pay and will forward the completed FORM SF-1190 to DFAS for processing.

(8) Repayment of the advance will be initiated by DFAS effective the first pay period after the employee reports to the foreign area duty station.

(9) It is the employee's responsibility to notify their respective FO in writing within 10 days, when any overpayment is received or an underpayment is made, and/or when appropriate deductions are not started/stopped as scheduled.

d. Use of Credit Cards. Employees are specifically precluded from using Government Contractor-Issued charge cards for PCS travel and PCS related costs, including expenses incurred during authorized HHT.

e. Obligation of Travel Funds. An employee may not, under any circumstances, obligate funds prior to the effective date indicated on the travel orders. Specifically, this precludes drawing advance funds to perform any official travel or permitting HHG to be shipped prior to the effective date of the orders.

f. Partial Settlement of Claims. Within 2 months of arrival at the new duty station, employees are advised to file a partial PCS settlement claim for HHT, travel and the first 30 days of TQSE. Amendments to the PCS claim for unknown/omitted expenses or any remaining real estate entitlements can be filed NTE 2 years after arrival at the new duty station. Amendments should be filed in a timely manner.

38-8. DEPENDENT TRAVEL

a. Some situations may dictate separate travel of dependents. These situations may include a dependent son or daughter attending college at the time of transfer, delay in selling a home, non-availability of quarters for dependents at the new duty station, etc. The PCS orders should list all qualified dependents as of the time the employee's travel will begin, regardless of whether travel of those dependents will be concurrent with the employee. Based on information provided in the travel questionnaire, separate travel for certain (or all) dependents will be authorized. Authorized transportation of dependents must begin within 2 years after the effective date of the employee's transfer.

b. In maternity situations, the travel questionnaire should note the anticipated delivery date. If this date precedes the scheduled date of transfer, the orders will include funding for the unborn child. Upon notification by the employee, the orders will be amended to include the child's name and date of birth.

c. As noted in Subchapter 38-22, dependent travel is not authorized if Separate Maintenance Allowance is authorized and paid.

38-9. HOUSE HUNTING TRIPS

a. For transfers within CONUS, NCIS employees may be authorized a government-paid round trip between the old and new duty stations to seek permanent quarters. This is not a blanket entitlement. When authorized, the employee or the spouse may undertake a House-Hunting Trip (HHT) alone or the employee may travel with his/her spouse. Reimbursable costs include a per diem allowance as well as transportation costs and a rental vehicle at the location of the new duty station. The HHT cannot exceed 10 consecutive calendar days, including travel.

b. Several factors must be considered and satisfied prior to approval of the HHT. These factors are:

(1) Based on family size, it may be less costly to the government and more convenient to the employee to complete arrangements for new quarters before the move.

(2) Conversely, the transfer of an employee who has no dependents will normally be accomplished at less cost to the government by authorizing a temporary quarters allowance at the new duty station.

(3) If government or other pre-arranged quarters are available at the new duty station, HHT will not be authorized.

(4) If the distance between the old and new duty station is less than 75 miles via surface route, HHT cannot be authorized.

(5) The transportation agreement must be signed prior to the authorization of a HHT.

c. As a general policy, the period authorized for temporary quarters will be reduced or avoided if a HHT has been authorized. Also, an extended temporary duty assignment at the new duty station or other circumstances may have provided adequate opportunity for the employee to complete arrangements for permanent quarters.

d. Authorization for the trip, mode of transportation, and period allowed will be included in the PCS orders. The employee will be in a duty status at no charge to leave during the authorized round trip period. Per diem costs during the HHT will be included in the travel advance of the PCS orders.

e. An employee's absence during a HHT should be recorded in the timekeeping system as ADLV.

f. There are two reimbursement options available to employees authorized HHT: actual expenses and fixed rate.

(1) The actual expense option is computed on the lodgings-plus method, i.e., the actual amount the traveler pays for lodging plus the applicable allowance for meals and incidentals, not to exceed the total maximum locality rate. The spouse is authorized 75% of such rate. The employee must itemize lodging expenses and provide receipts for lodging.

(2) The fixed rate option is computed by multiplying the locality rate by 6.25 if the employee and spouse both travel (either together or separately), or, if only one travels, multiplying the locality rate by 5. When an employee elects to be reimbursed using the fixed rate, no itemization or receipts are required.

g. The employee is not obligated to accept the offer of a fixed rate reimbursement. He/she may decline the offer and choose to be reimbursed by the actual expenses option. However, once the employee selects a reimbursement method and annotates the travel questionnaire accordingly, the selection cannot be changed.

38-10. TEMPORARY QUARTERS SUBSISTENCE EXPENSES

a. Section C13000 of the JTR Vol II provides for reimbursement of certain subsistence expenses incurred in connection with a PCS. Subsistence expenses include the cost of lodging, meals, groceries, incidental tips and fees. TQSE can only be authorized if the new duty station is located in the United States or in a non-foreign (OCONUS) area.

b. TQSE will not be authorized when a change in duty station would increase the employee's usual one-way commuting distance (old residence to old duty station) by 50 miles or less (old residence to new duty station).

c. As a general rule, the location of the temporary quarters must be within reasonable proximity to the old or new official duty station. Payment of subsistence expenses for occupancy of temporary quarters in other locations will not be allowed unless justified by circumstances unique to the individual employee or the employee's dependents that are reasonably related and incident to the transfer. Occupancy of temporary quarters will not be approved for vacation purposes or other reasons unrelated to the transfer.

d. TQSE must begin no later than 2 years after the employee reports for duty at the new duty station, unless an extension is approved by Code 10A.

e. The period of time allowed for TQSE will run concurrently for the employee and all dependents. The consecutive period of days may be interrupted for actual travel time between the old and new duty stations and for intervening temporary duty assignments. However, in the latter situation, if dependents occupy temporary quarters while the employee is TDY, the period of days authorized for TQSE will not be interrupted. TQSE may be reimbursed while the employee is on annual leave provided the leave does not delay termination of temporary quarters and occupancy of a permanent residence at the new duty station.

f. Extensions of TQSE may be authorized only in situations where there is a demonstrated need for additional time in temporary quarters due to circumstances which have occurred during the initial 60-day period of temporary quarters occupancy and which are determined to be beyond the employee's control. Examples of compelling reasons could include delay in shipment and/or delivery of household goods; delay in availability of new permanent residence because of unanticipated problems (e.g., delays in settlement on new residence, short term delays in construction of a new residence, inability to locate a permanent residence which is adequate for family needs because of housing conditions at the new official station; sudden illness, injury, or death of employee or immediate family member.)

g. If an employee, during the initial 60 day-period of temporary quarters, enters into a contract for a residence which indicates a settlement date after the initial 60-day period, the situation is not normally considered to be beyond the employee's control and an extension of TQSE might not be authorized.

h. There are two types of calculations/reimbursement for TQSE expenses: fixed rate and actual expenses. As with the HHT, the employee is not obligated to accept the offer of fixed rate

TQSE. However, once the employee selects a TQSE payment method and annotates it on the travel questionnaire, the selection may not be changed.

(1) The fixed rate TQSE allowance is a lump-sum payment and does not require receipts or supporting statements. It is limited to 30 days and cannot, under any circumstances, be extended. For computation purposes, the employee is authorized 75% of the applicable locality (high cost) or overseas per diem rate for the number of days of fixed TQSE, not to exceed 30 days. Dependents, regardless of relationship or age, are authorized 25% of the employee's rate for the number of days of fixed TQSE, not to exceed 30 days.

(2) The actual expense TQSE is normally authorized for an initial 60-day period. If compelling reasons exist, the total period of actual expense TQSE may be extended for up to an additional 60 days. Under no circumstances can the actual expense TQSE be extended beyond 120 days. For computation purposes, the employee is authorized either the CONUS per diem rate or the overseas per diem rate for the first 30 days. The spouse and dependents over age 12 are authorized 75% of the rate and dependents under age 12 are authorized 50% of the rate. For additional periods beyond the initial 30 days, the employee is authorized 75% of the CONUS per diem rate. The spouse and dependents over age 12 are authorized 50% of the rate and dependents under 12 are authorized 40% of the rate.

(3) Claims for Fixed Rate TQSE should be submitted to Code 10A using Standard Form 1351-2. Claims for actual subsistence expenses should be submitted to Code 10A using the TQSE Form.

38-11. TEMPORARY QUARTERS SUBSISTENCE ALLOWANCE

a. Civilians transferring to and from foreign areas are entitled to a Temporary Quarters Subsistence Allowance (TQSA). The TQSA is intended to assist in covering the average cost of adequate but not elaborate or unnecessarily expensive accommodations in a hotel, pension, or other transient-type quarters at the post of assignment, plus reasonable meal and laundry expenses. The TQSA covers those expenses incurred by the employee and/or family members for up to 90 days after arrival at the foreign post, and up to 30 days preceding final departure from the foreign area.

b. The DOS Standardized Regulation (DSSR) is the authority for reimbursement of certain expenses incurred in a foreign area.

(1) Arrival At Foreign Post: TQSA stops and Living Quarters Allowance (LQA) becomes payable when the employee changes from temporary lodging and occupies permanent quarters or at the end of 90 days after arrival in theater, whichever is sooner.

(2) Departure From Foreign Post: At the end of the tour, TQSA is payable after vacating permanent quarters or termination of LQA, and entering temporary quarters, but not earlier than 30 days prior to employee departing the post. Use of the TQSA at the end of a foreign tour is intended to allow early shipment of household goods, so as to minimize delay in setting up quarters at the new permanent duty station.

(3) The 90 and 30 day periods may be extended up to but not more than an additional 60 days in each case if it is determined by Code 10A that compelling reasons beyond the control of the employee require continued occupancy of temporary quarters.

(4) The amount of TQSA to be reimbursed will be the lesser of either the actual amount of allowable expenses incurred or the amount computed as follows:

(a) First 30 days upon arrival or 30 days preceding final departure: For the employee, 75% of the per diem rate for the foreign area as listed in the DSSR; 50% of the employee's rate for each family member age 12 or over; 40% of the employee's rate for each family member under age 12.

(b) Second 30 days upon arrival or first 30 day extension preceding final departure: For the employee, 65% of the per diem rate for the foreign area as listed in the DSSR; 45% of the employee's rate for this period for each family member age 12 or over; 35% of the employee's rate for this period for each family member under age 12.

(c) Third 30 days upon arrival or second 30 day extension preceding final departure: For the employee, 55% of the per diem rate for the foreign area as listed in the DSSR; 40% of the employee's rate for this period for each family member age 12 or over; 30% of the employee's rate for this period for each family member under age 12.

(d) Additional 60 days upon arrival at the new foreign duty station - computed at the same rates established above for the third 30-day period.

(5) TQSA is not included in the actual PCS orders; instead, reimbursement is effected through use of FORM SF-1190, Statement of Actual Expenses and a TQSA Expense Worksheet, DSSR-120. Lodging and dry cleaning receipts are also required.

(6) The completed forms and receipts should be forwarded via the Field Office to Code 10A for processing through DFAS.

(7) An advance of funds for TQSA may be made in 30-day increments. The initial advance shall not exceed the maximum amount allowable for the first 30-day period. Thereafter, funds may be advanced for subsequent 30-day periods not to exceed the maximum amount for each period.

(8) An employee receiving TQSA is required to file reconcilement paperwork with Code 10A via their Field Office, in a timely manner, but NLT 6 months after arrival at the new duty station.

38-12. FOREIGN TRANSFER ALLOWANCE

a. Employees and their dependents transferring from a duty station in the 50 states or the District of Columbia to a duty station in a foreign area are eligible for Foreign Transfer Allowance (FTA). FTA applies to lodging, meals, laundry, cleaning and pressing while in

temporary quarters. The allowance is authorized for a period of up to 10 days and must be used prior to final departure from the 50 states or the District of Columbia and not more than 30 days after vacating permanent residence quarters.

b. The initial occupant, whether the employee or a dependent age 12 or over, is authorized a daily rate not in excess of the applicable locality rate for the old duty station. For each additional occupant, whether the employee or a dependent age 12 or over, two thirds of the daily rate established for the initial occupant is authorized. For each additional occupant under age 12, the daily rate is one half of the rate established for the initial occupant.

c. An estimate of FTA expenses will be included in the PCS orders and is also included in the Travel Advance.

d. Claims for Fixed Rate FTA should be submitted using the SF-1190 with lodging and dry cleaning receipts attached.

38-13. LIVING QUARTERS ALLOWANCE (LQA)

a. The Living Quarters Allowance (LQA) is intended to reimburse an employee for substantially all costs for residence quarters when Government-owned or Government-leased quarters are not provided. The LQA includes rent, plus any additional costs for heat, light, heating fuel, gas, electricity, water, taxes levied by the local government and required by law or custom to be incurred by landlord and paid by lessee. Employee may also be reimbursed for garage space for one automobile NTE 25% of the flat rate authorized for the employee. In order to be eligible for agent's fee reimbursement, the agent's fee must be paid by the lessee to the landlord who is obligated to pay the fee and must not be paid by the lessee directly to the agent. LQA and TQSA cannot be paid to an employee simultaneously.

b. The following costs may not be included in rent: (1) concierge or notary's fees; (2) agent's fee except under conditions noted in paragraph 38-11.1 above; (3) telephone installation or maintenance; (4) deterioration of property or furnishings; (5) servant's wages or maintenance; (6) tips; (7) cleaning; (8) storage; (9) garden or lawn service; (10) servants' quarters, unless considered part of the same property with the living quarters; (11) garbage or trash disposal; and (12) any other extraneous expenses not directly related to rent.

c. The LQA will become effective on the date the employee moves into permanent quarters in a foreign area (but not later than 90 days). Changing to LQA status terminates TQSA benefits. Upon departing a foreign area, the LQA will terminate on the date the employee moves from permanent quarters into temporary quarters, when TQSA benefits again become available.

d. Advance Payment of LQA may be made in localities where local custom necessitates the advance payment for periods of at least three months and where the individual lessor requires the customary advance payment of rent. The amount that may be paid in advance shall be for a period of not less than 3 months or not more than 2 years. Requests by the employee for advance LQA must be coordinated via the NCIS Field Office (NCISFO). The NCISFO must notify Code

10A in order to process the request and must notify Code 14 of the advance funding request and amounts involved.

e. LQA is governed by the DSSR, and is subject to change. As with other foreign area entitlements, changes, advances and reimbursement of LQA are effected through use of FORM SF-1190 and the LQA Worksheet, FORM DSSR 130. SF-1190s for all employees transferring to foreign areas will be processed through the FO to Code 10A for payment through DFAS.

f. Any change in the expenses, which would affect LQA payments, must be reported by the employee to the NCISFO in a timely manner, i.e., within 10 days, utilizing a SF-1190 with necessary supporting documentation.

g. Employee is responsible for notifying the NCISFO, via e-mail or in writing, within 10 days, of any under-payments, duplicate payments, or over-payments of overseas benefits by DFAS. Employee is also responsible for timely settlement of any overpayments received. The NCISFO must track overpayment/underpayment issues through final reconciliation, ensuring timely settlement. The NCISFO will keep Code 14 advised of the situation.

h. The State Department requires a reconciliation filing of FORM SF 1190 for LQA benefits at the end of the first year. NCISHQ Code 10A is the POC for this review and will provide instructions on reporting requirements and deadlines. Employees receiving LQA must meet the requirements and deadlines imposed by NCISHQ Code 10A. Note: The annual reconciliation of overseas benefits process will result in recoupment/reimbursement of any minor underpayments or overpayments adjustments.

38-14. OVERSEAS POST ALLOWANCE

a. The overseas post allowance is established for certain overseas locations, to permit employees to spend the same portion of their basic compensation on current living expenses as they would in Washington DC, without incurring a reduction in their standard of living due to higher costs for goods and services at their assigned post.

b. Post allowance is not authorized at all locations. As with other allowances, the post allowance is subject to change, or discontinuation at any time, without advance notification. The amount, date of change or discontinuation is specified by the State Department. Usually, by the time DFAS receives notification, the effective date is retroactive, and therefore pay adjustments (plus or minus) will be made to the employee's post allowance pay.

c. Post allowance starts when an employee terminates TQSA. When the employee is transferred from the overseas post, the post allowance terminates upon entering TQSA status. Post allowance benefit application is included on the SF1190 filed at the time the employee switches from TQSA to LQA status, or the FORM SF1190, filed when the employee terminates LQA status and enters TSQA status. Post allowance and TQSA cannot be paid simultaneously. The NCISFO will forward the completed paperwork to NCISHQ Code 10A. After confirming requested benefits, Code 10A will forward instructions to DFAS, and the employee's bi-weekly pay and allowances will be adjusted, as necessary.

d. Overpayment/Underpayment of Post Allowance: If an employee becomes aware of any overpayment or underpayment of post allowance benefits in his/her LES, it is incumbent upon that employee to notify the Field Office, in writing, within 10 days of receipt of underpayment/overpayment. The Field Office will track the problem through final reconciliation with DFAS and keep Code 14 apprised of the situation.

e. Post Allowance can be paid to both members of a married couple when eligible based on their position (some local hires are not eligible for post allowance per DSSR **Subchapter 220**) whether or not one spouse is military. Each one may only claim for one person and any dependents will need to be assigned to one or the other, but not both.

38-15. REAL ESTATE BENEFITS

a. The JTR provides for compensation for most expenses incident to the sale or purchase of a residence provided the old and new duty stations are located within the United States, Commonwealth of Puerto Rico, or the Commonwealth of the Northern Mariana Islands.

b. Employees will be entitled to reimbursement for some of the incidental expenses incurred in connection with the sale of a residence at the old duty station, the purchase of a residence at the new duty station, or the settlement of an unexpired lease involving the house or apartment, or a lot on which a mobile home, used as the residence, was located at the old duty station. Please see paragraphs 38-13.6 for a list of reimbursable expenses. Please also see paragraphs 38-13.4, 38-13.5, and 38-13.7 for limitations on and exclusions from reimbursement. Please also note that the entitlement exists only after the required transportation agreement has been signed.

c. Additionally, there are instances when an employee completes a tour of duty in a foreign area and is subsequently transferred to a different official duty station in a non-foreign area (not the one from which he/she transferred when assigned to the foreign post of duty). When this type of transfer is authorized or approved, reimbursement is allowable for incidental real estate expenses required to be paid by the employee in connection with:

(1) The sale of the residence (or the settlement of an unexpired lease) at the official station from which the employee was transferred when he/she was assigned to a duty station located in a foreign area; and

(2) The purchase of a residence at the new official station. It is not necessary for an employee to sell a residence to be eligible for reimbursement of incidental expenses for the purchase of a residence.

d. Limitations on the amount of reimbursement are:

(1) In connection with the sale of the residence at the old duty station - 10% of the actual sale price (there is no monetary cap associated with this entitlement).

(2) In connection with the purchase of a residence at the new duty station - 5% of the purchase price (there is no monetary cap associated with this entitlement)

e. Settlement dates for the sale and purchase or lease termination transactions for which reimbursement is requested must not be later than 2 years after the date that the employee reported for duty at the new permanent duty station. Upon the employee's written request, the 2-year time limitation may be extended for an additional period of 2 years if there are extenuating circumstances, which precluded the employee from completing the real estate transactions within the prescribed timeframe. However, the employee's written request must be submitted to Code 10A as soon as the employee becomes aware of the need for an extension but before expiration of the 2-year limitation.

f. Reimbursable expenses include the following:

(1) A broker's fee or real estate commission paid by the employee for services in selling his/her residence at the old duty station. (No such fee or commission is reimbursable in connection with the purchase of a home at the new duty station.)

(2) Advertising and selling expenses, such as costs of newspaper, bulletin board, multiple-listing services, or other advertising if such services have not already been paid in the form of a broker's fee or commission. The customary cost of appraisal is also reimbursable.

(3) Legal and related costs, to the extent such costs have not been claimed under other categories, including: costs of searching title, preparing abstract and legal fees for a title opinion, or where customarily furnished by the seller, the cost of a title insurance policy; cost of preparing conveyances, other instruments, and contracts; related notary fees and recording fees; and cost of making surveys, preparing drawings or plats when required for legal financing purposes. (Costs of litigation are not reimbursable.)

(4) Miscellaneous expenses, generally those customarily paid in the locality of the residence, include: FHA or VA fee for the loan application; loan origination fees and similar charges such as loan assumption fees and loan transfer fees; cost of preparing credit reports; mortgage and transfer taxes; state revenue stamps; charge for prepayment of a mortgage or other security instrument that includes a prepayment charge mortgage title insurance policy paid by the employee for the protection of, and required by, the lender; owner's title insurance policy, provided it is prerequisite to financing or the transfer of property, or the cost of the owner's title insurance policy is inseparable from the cost of other insurance, which is a prerequisite to financing or the transfer of property; and expenses in connection with construction of a residence, which are comparable to expenses that are reimbursable in connection with purchase of an existing residence.

(5) The following items of expenses are not reimbursable:

(a) Owner's title insurance policy, "record title" insurance policy, mortgage insurance or insurance against loss or damage of property, and optional insurance paid for by the employee in connection with the purchase of a residence for the protection of the employee.

(b) Interest on loans, points, and mortgage discounts.

(c) Property taxes.

(d) Operating or maintenance costs.

(e) No fee, cost, charge or expense determined to be part of the finance charge under the Truth in Lending Act, Title I, P.L. 90-321, and Regulation Z, issued in accordance with P.L. 90-321 by the Board of Governors of the Federal Reserve System, unless specifically authorized above.

(f))Expenses that result from construction of a residence.

(g) VA funding fee.

(h) Funds required for down payment or mortgage payments.

38-16. RELOCATION SERVICES CONTRACT

a. DoD components are authorized to enter into contracts with private firms to provide relocation services to designated employees. The primary service provided is that of the guaranteed home sale at the old duty station.

b. The Department of the Navy (DON) has contracted for relocation services for certain categories of its military and civilian employees. Within NCIS, the following categories of employees are eligible for these services:

(1) All Senior Executive Service members.

(2) All employees relocating under mobility agreements, regardless of grade.

c. The general conditions and limitations for eligibility for relocation services are that the employee's transfer is in the interest of the government and it is not primarily for the convenience or benefit of the employee or at the employee's request. An employee who is authorized services under the contract continues to be entitled to relocation allowances under the JTR; however, dual benefits are prohibited.

d. NCISHQ Code 10A maintains central control for the ordering of relocation services through a Relocation Services Coordinator. Employees interested in the service must sign a transportation agreement and request that an order for a contract be placed via the coordinator. NCIS policy requires that an employee list their residence for sale for 60 days prior to contracting for relocation services.

e. Home Marketing Incentive. The JTR provides a home marketing incentive payment for transferring employees authorized to participate in the relocation services program. The purpose of the incentive is to encourage employees to independently and aggressively market, and find a bona fide buyer for, their residences. As a result, the DON pays a significantly reduced fee for services to the relocation services company. To qualify for the incentive, the employee must actively list the residence for 60 days. If the employee has not sold the residence at the end of the 60-day period, he/she may enter the residence in the DoD's home sale program. If the employee is then able to locate a buyer, the residence is transferred to the relocation services company through which the buyer completes the sale.

f. The maximum amount payable for the home marketing incentive may not exceed the lesser of:

(1) Five percent of the price the relocation services company paid when it purchased the residence for the employee (Example: The relocation services company gives the employee a buyout offer of $150,000 for the residence; 5% incentive would be $7,500.)

(2) $10,000; or

(3) One-half of the savings realized from the reduced fee/expenses paid as a result of the employee finding a bona fide buyer when the sale is closed. If no savings are realized, a home marketing incentive may not be paid.

g. Eligible employees requesting authorization for the home marketing incentive must do so in writing. Included in the request must be the dates that the residence was listed, the date the employee transferred to the relocation services company and the name of the buyer. Necessary information may be provided by e-mail to NCISHQ Code-10A.

38-17. PROPERTY MANAGEMENT PROGRAM

a. The employee covered by a mobility agreement who is transferred to a new permanent duty station (PDS) and who is eligible to sell a permanent residence at the old duty station, may be eligible for property management (PM) services. PM services assist in offsetting costs associated with retaining a residence at the old PDS. The employee and/or a member of the employee's immediate family must hold title to the residence. Payment for PM services under this section shall not exceed 2 years from the effective date of the employee's transfer.

b. Authorized PM services shall be obtained through the relocation services program. Typical PM services include:

Obtaining a tenant;
Negotiating the lease;
Inspecting the property regularly;
Managing repairs and maintenance;
Enforcing lease terms;
Collecting the rent;

Paying the mortgage and other carrying expenses from proceeds and/or the employee's funds;
Accounting for the transactions and providing periodic reports to the employee; and
Similar services.

c. An employee is taxed on the amount of PM services expenses the Government pays a relocation services company or reimburses directly to the employee. The employee will receive a Relocation Income Tax (RIT) allowance for the additional Federal, State, and local income taxes incurred on PM services expenses. Employees should consult a tax advisor for specific details on the tax liability resulting from the use of PM services.

d. Employees opting to use PM services, who later decide to sell the residence, are subject to the 2-year limitation for the sale of a permanent residence at Government expense. The total expense may not exceed the maximum amount allowed for the sale of a residence, less the amount paid for PM services.

38-18. MISCELLANEOUS EXPENSE ALLOWANCE

a. The miscellaneous expense allowance is provided to defray various contingent costs associated with relocation of a residence in connection with a PCS. An advance of funds for miscellaneous expenses can be authorized 3 weeks prior to the PCS move.

b. Reimbursable items include, but are not limited to, the following:

(1) Disconnecting and connecting appliances, equipment and utilities involved in relocation, and the cost of converting appliances for operation on available utilities (this does not include the cost of purchasing appliances or equipment in lieu of conversion);

(2) Cutting and fitting rugs, draperies and curtains moved from one residence quarters to another;

(3) Utility fees or deposits that are not offset by eventual refunds;

(4) Forfeiture or losses on medical, dental, or related contracts, and contracts for private institutional care, such as that provided for handicapped or invalid dependents, which are not transferable or refundable;

(5) Automobile registration, driver's license and use taxes imposed when bringing automobiles into some jurisdictions, cost of reinstalling a catalytic converter upon reentry of vehicle into the U.S. for employees participating in the DoD POV Import Control Program; cost of securing a bond allowing a POV to be admitted into the U.S. for non participants in the DoD POV Import Control Program.

(6) Rental agent fees customarily charged for securing housing in foreign countries.

c. Expenses that are not reimbursable under the miscellaneous expense allowance include:

(1) Losses in selling or buying homes and personal property and cost items related to such transactions;

(2) Duplication of payments for otherwise reimbursable expenses;

(3) Cost of additional insurance on household goods while in transit to the new duty station, or cost of loss or damage to such property;

(4) Additional costs of moving household goods caused by exceeding the maximum weight limitation for which the employee has eligibility as provided by law or in the JTR, Vol II;

(5) Higher income, real estate, sales, or other taxes as the result of establishing residence in the new locality;

(6) Fines imposed for traffic infractions while en route to the new duty station;

(7) Accident insurance premiums or liability costs incurred in connection with travel to the new duty station locality, or any other liability imposed upon the employee for uninsured damage caused by accidents for which the employee or the employee's dependents are held responsible;

(8) Losses as the result of the sale or disposal of items of personal property not considered convenient or practicable to move;

(9) Damage to or loss of clothing, luggage, or other personal effects while traveling to the new duty station;

(10) Subsistence, transportation, or mileage expenses in excess of the amounts reimbursed as per diem or other allowances under the provisions of the JTR, Vol. II;

(11) Medical expenses due to illness or injuries of the employee or his/her dependents while en route to the new duty station or while living in temporary quarters;

(12) Costs incurred in connection with structural alterations; remodeling or modernizing of living quarters, garages, or other buildings, to accommodate privately owned automobiles, appliances or equipment; or the cost of replacing or repairing worn out or defective appliances or equipment shipped to the new location;

(13) Costs of purchasing clothing, appliances, and equipment incident to relocation;

(14) Costs of newly acquired items, such as the purchase or installation cost of new rugs or drapes.

d. Miscellaneous expense allowance is authorized as follows:

(1) $1000.00 or the equivalent of two weeks' basic pay, whichever is less, is authorized for an employee with dependents;

(2) $500.00 or the equivalent of one week's basic pay, whichever is less, is authorized for an employee without dependents.

(3) The $1000 and $500 amounts may be paid without being supported by receipts or itemized statements.

(4) These amounts may be increased upon written request of the employee, provided the aggregate amount does not exceed the employee's basic salary rate for two weeks if the employee has dependents, or one week without dependents. If this maximum amount is claimed, the claim must be supported by paid bills, receipts or other acceptable evidence justifying the entire amount claimed.

38-19. TRANSPORTATION OF HOUSEHOLD GOODS

a. Government Bill of Lading (GBL). A GBL is a document showing shipment of HHG and an acknowledgement of their receipt. This differs from a commercial bill of lading primarily in that the government acts as the contracting party with a commercial carrier. Shipment of HHG via GBL is normally more convenient to the employee in that the GBL includes packing by the carrier. Overseas shipments are by GBL only. All NCIS PCS orders will contain a provision authorizing shipment of HHG via GBL. However, JTR Vol II specifies that the local transportation officer must determine that shipment of HHG via GBL (vs. commuted rate) is more advantageous to the government by at least $100.00. NCISHQ cannot direct CONUS shipment via GBL; it can merely authorize it.

b. Commuted Rate. If an employee chooses to negotiate with a commercial carrier to ship their HHG, the amount that may be reimbursed will be determined by "commuted rate" tables. Commuted rate is a specified dollar amount based on the weight of the HHG and the distance involved. The distance is determined by mileage guides filed with the Interstate Commerce Commission. If the rate is not indicated for the exact mileage, the rate for the next greatest distance shall apply. If the weight transported is less than the lowest minimum weight provided in the rate table, the reimbursement shall be based on the lowest minimum weight provided in the rate table instead of the actual weight transported.

c. Weight Allowances. The maximum weight allowance for HHG shipment is 18,000 pounds net for all civilian employees. Travel orders will specify shipment in net weight and cannot exceed this maximum. If both husband and wife in the same household are employees, transportation of HHG applies to either, provided there is no duplication and the maximum weight allowance is not over 18,000 pounds net for the household.

(1) For movement to and between overseas activities, maximum weight allowances may vary. When public quarters or private housing include Government-owned furnishings, shipment of HHG at Government expense to and from such stations is limited to 4,500 pounds

(net weight). The remainder of the employee's HHG may be placed in non-temporary storage at government expense. This weight limitation is exclusive of the weight of unaccompanied baggage. When any item of government-owned furnishings which is normally provided is unavailable, and the employee is so advised, the allowance will be increased in an amount equal to the weight of personally owned furnishings required in lieu of the unavailable items. The total net weight of HHG stored and HHG shipped cannot exceed 18,000 pounds.

(2) When HHG are shipped uncrated, as in a household mover's van or similar conveyance, the net weight shown on the bill of lading or on the weight certificate will include the weight of barrels, boxes, cartons and similar materials used in packing. It will not include pads, chains, dollies and other equipment needed to load and secure the equipment.

(3) When property is transported crated, the net weight will not include the weight of the crating material. The net weight will be computed as being 60% of the gross weight. However, if the net weight computed in this manner exceeds the applicable weight limitation and if it is determined that, for reasons beyond the employee's control, unusually heavy crating and packing materials were necessarily used, the net weight may be computed at less than 60% of the gross weight.

(4) When special containers designed normally for repeated use, such as lift vans, CONEX transporters, and HHG shipping boxes, are used and the known tare weight does not include the weight of interior bracing and padding materials but only the weight of the container, the net weight of the HHG shall be 85% of the gross weight less the weight of the container. If the known tare weight includes interior bracing and padding materials so that the net weight is the same as it would be for uncrated shipments in interstate commerce, the net weight shall not be subject to the weight reduction.

(5) With regard to professional books and papers and equipment, there is no statutory authority to transport such personally owned items in addition to the maximum weight of HHG. When the additional weight of personally owned professional books, papers, and equipment would result in an excess of the authorized weight allowance for HHG to be shipped, they must be transported to the new permanent duty station as an administrative cost, not chargeable to the appropriations available for travel and transportation expenses. To utilize this authority, an administrative certification must be furnished by the SAC of the new field office or the appropriate EAD/AD/DAD at NCISHQ, that the books, papers, and equipment are necessary in the proper performance of the employee's duty at his/her new station, and that similar books, papers and equipment would have to be obtained at government expense for the employee's use if they were not transported to the new duty station. Furthermore, the PCS orders must specifically authorize the shipment of professional items and the GBL must reflect separate appropriation data.

(6) Insurance Information. Loss of or damage to HHG, privately owned vehicles and other personal property shipped under orders, in conjunction with travel under orders, is reimbursable under the provisions of the Military Personnel and Civilian Employee's Claims Act of 1964. A more complete description of this coverage can be found in the Insurance Information Sheet. It would be wise to take photographs of all personal possessions. Normally,

movement of HHG in a PCS move takes place without significant incident. A few NCIS personnel have, however, experienced some severe losses. While their goods were insured, the absence of detailed inventories delayed settlement and made a bad situation worse. It is strongly recommended that an inventory record be prepared, either written, tape recorded, photographed or a combination, and shipped separately to the new PDS.

(7) Carrier Recovery Claims. To recover funds for the loss or damage of HHG, the carrier will complete a DD Form 1840, which will include the address of its office for receipt of notice. The delivery agent will present the form to the employee at delivery. The employee will list damage and loss noticed at delivery on the DD Form 1840 and will sign acknowledging receipt of three copies of the form. The employee retains the form and is instructed, by the form, to list all later noticed loss and damage on the reverse side (the DD Form 1840-R) and to deliver two copies of the form within 70 days from the date of delivery to the office designated within a local area to receive HHG shipment claims. The claims office has until 75 days after delivery of the employee's property to issue notice (i.e., 5 days to process a form delivered on the 70th day). If no form is received by the employee, the Government has no time limit within which it must notify the carrier of additional loss and damage. One copy of the form is mailed to the carrier for processing. The claims office retains the other copy.

(8) Items Of Extraordinary Value. Items of extraordinary value include such things as articles of gold and other precious metals, jewelry, valuable art, rare collections, etc. These and other items of substantial value usually worn or carried by the employee or his/her family (such as cameras and accessories, binoculars, jewelry, including costume jewelry etc.) that are prone to pilferage when shipped by ordinary modes may be shipped by the expedited mode of transportation that will produce the lowest overall cost to the government and which will provide satisfactory service. The responsible Transportation Officer will select the appropriate expedited mode of travel. The net weight of such shipments will be charged against the employee's total weight allowance.

d. Storage Of Household Goods

(1) Temporary Storage: The time allowable for temporary storage in connection with an authorized shipment of household goods is 90 days. However, upon an employee's written request, the initial 90-day period may be extended for an additional 90-day period not to exceed a total of 180 days under certain conditions if approved by NCISHQ. Storage may be at point of origin, destination, en route, or any combination thereof.

(2) Non-temporary Storage. For an employee stationed at, transferred to, or appointed for assignment to an overseas permanent duty station, one of the following conditions must be met in order to be eligible for non-temporary storage:

(a) The permanent duty station is one to which the employee cannot take or cannot use his/her household goods;

(b) The storage is authorized in the public interest;

(c) The estimated cost of storage would be less than the cost of round trip transportation (including temporary storage) of the HHG to the new permanent duty station.

(3) Non-temporary Storage Policy.

(a) HHG may be stored in available Government-owned storage facilities or in suitable privately-owned facilities obtained by the Government. The transportation officer will determine which storage facilities will be used. Storage at Government expense may be authorized for a period not to exceed the length of the tour of duty plus one month prior to the time the tour begins.

(b) New fiscal year accounting data is required each year to extend the non-temporary storage of HHG at government expense. Accordingly, it is important that the following information be provided to NCISHQ Code 10A at the time of storage: amount of HHG placed in storage, lot number and name and address of storage facility. This information may be provided by GEN, fax, or e-mail.

38-20. TRANSPORTATION OF PRIVATELY OWNED MOTOR VEHICLES

a. Transportation of a privately owned motor vehicle (POV) at government expense is not authorized when the motor vehicle may be driven to the new duty station over hard-surfaced all-weather highways, including ferries. For in-CONUS moves, the employee will be authorized a mileage allowance together with related per diem and travel time to transport the vehicle from the old to the new permanent duty station. Although leave enroute is frequently requested and results in a more circuitous route, reimbursement will be set/fixed by the most direct route. In those instances where the number of authorized dependents or amount of personal possessions precludes transportation by only one vehicle, reimbursement for additional vehicles may be authorized.

b. For overseas moves, transportation at Government expense is limited to vehicles having a gross size for shipping purposes of not more than 20 measurement tons (800 cubic feet). An employee who ships a larger vehicle which otherwise qualifies for shipment at government expense must pay all costs which result from the excess size of the vehicle. When delivered at the shipping point, the vehicle should be in good operating condition with all required equipment (i.e., exhaust system, windshield, headlights, etc.) in sound mechanical condition. The body should be free of any breaks or tears. A complete set of keys must accompany the vehicle when it is turned in. Tools, hubcaps and any other items that could be damaged easily or stolen should be boxed and placed in the vehicle's trunk. Finally, inspect the vehicle carefully prior to turn-in so that any damage in transit can be documented. For additional information, refer to the Checklist_for_Shipment_of_POV.

c. The transportation officer is responsible for designating the shipping point to be utilized. A list of the shipping points within CONUS is attached. The employee is responsible for transporting the POV to the shipping point. One-way mileage to the port facility and the actual cost incurred for one-way return transportation to the duty station will be authorized. When an employee reclaims his vehicle at a port facility, one-way transportation to the port and

one-way return mileage will be authorized. Per Diem is not a reimbursable expense in either situation.

d. The shipment of an employee's POV to an overseas duty station may be authorized when it is in the interest of the government for the employee to have the use of a motor vehicle at the post of duty. Use of the POV primarily for the convenience of the employee and his/her immediate family does not constitute interest of the government. It may be deemed to be in the interest of the government if:

(1) The use of the POV will contribute to the employee's job effectiveness;

(2) The use of a POV of the type involved will be suitable in the local conditions of the official station;

(3) Local conditions at the new station make it desirable from the government's viewpoint for the employee to have the use of a POV;

(4) Transportation costs of the POV will not be excessive;

(5) The POV is of U.S. manufacture unless the Commanding Officer determines that only a foreign made POV may be effective and the POV was purchased in advance of the transfer notification.

(6) Shipment of an employee's POV to overseas area is not based primarily for the convenience of the employee and his/her immediate family.

e. When the determination has been made that the shipment of a POV is in the interest of the government, the transportation of the POV to an official station outside of CONUS will be authorized on the PCS orders. Leased vehicles will not be authorized for shipment. A POV may be transported to the U.S. when its use is no longer required at a station outside CONUS. An employee who is being transferred from an overseas post to CONUS may have his/her POV shipped to CONUS provided the POV was transported at government expense to the overseas post. Transportation of a POV from an overseas duty post may also be authorized if the POV to be shipped is a replacement for a POV that was shipped overseas. It is reiterated that, in those instances where an employee did not ship a POV to the overseas duty post, there is no entitlement for return shipment of a POV to CONUS. The POV must meet emission and other standards imposed by JTR regulations, prior to shipment to CONUS.

f. The transportation at government expense of a POV of foreign manufacture (FPOV) in connection with permanent change of station orders is prohibited unless the FPOV was purchased as a replacement for a vehicle that was shipped at government expense to an overseas area listed in the JTR Vol II that is exempt from the prohibition on shipment of FPOV. Transportation of such a FPOV will not be authorized at government expense if the FPOV was purchased less than one year before the effective date of the employee's permanent change-of-station. An exception to this restriction may be granted if the overseas commander

concerned substantiates that the vehicle purchased replaces a vehicle which was lost or destroyed through fire, theft, accident, rapid deterioration, or is not repairable.

g. One POV may be shipped to the employee's overseas permanent duty station as an emergency replacement for the first motor vehicle within a period of four years from the date the first motor vehicle was shipped overseas. Before the shipment of an emergency replacement vehicle may be authorized, it is necessary that 0010A ascertain that the replacement vehicle is necessary for reasons beyond the control of the employee, such as loss or destruction of the first vehicle through fire, theft, accident, rapid deterioration due to severe climatic conditions at the station, or similar causes, and, in addition, a determination that the replacement vehicle is in the interest of the government. A shipment of one emergency replacement vehicle may be authorized during each succeeding four-year period of continuous permanent duty assignments at a permanent duty station outside CONUS.

38-21. RENEWAL AGREEMENT TRAVEL (Overseas only)

a. Employees are entitled to renewal travel at government expense upon completion of their overseas tour provided a new tour has been approved and the employee signs a Transportation Agreement for a Renewal Tour to immediately follow the completed tour. Initial tour lengths and renewal tour lengths are prescribed in the JTR. Orders are prepared by Code 10A based upon an abbreviated travel questionnaire submitted via the FO. Information on the travel destination, dates of travel, and family members accompanying sponsors will be required to prepare orders.

b. Family members do not have to perform Renewal Travel concurrently with the employee. They may travel separately provided travel is performed within 6-months of the employee's travel. However, if the employee does not elect to perform renewal travel, dependents have no entitlement to such travel. Dependents who turn 21 years of age overseas will be authorized one-way travel to CONUS on the Renewal Orders.

c. If an employee's renewal tour is at the same duty station as the initial tour, the employee may request (through Code 10A, with SAC approval) authority to perform travel slightly earlier or later than it would normally be scheduled. Usually this is done to coincide with the start or end of the school year or other family considerations. If an earlier/later date is approved the following changes will be made without impacting the tour rotation date:

(1) The initial tour will be administratively extended or reduced, as appropriate.

(2) The renewal tour will be administratively extended, or reduced, as appropriate.

d. Adjustment of tours cannot be accommodated when the employee travels to a new duty station after renewal travel. Such travel is considered an actual PCS move which involves other JTR rules.

e. Renewal travel is normally to the employee's place of actual residence, or Home of Record. This does not necessarily mean the last duty station, but may be some other location

where the employee has a residence, pays taxes, etc. This location should be noted on the Transportation Agreement at the time the employee transfers to the overseas post. If the employee elects to travel to an alternate location, the orders will be prepared to reflect travel at "constructive cost", i.e., reimbursement for travel will be limited to the cost associated with travel to the Home of Record. Employees may purchase their own airline tickets for personal convenience provided they are aware that reimbursement is limited to constructive cost of government air transportation.

f. Renewal travel benefits cannot be accumulated and rolled over from one renewal tour to another consecutive tour, i.e., if not utilized in first renewal tour, two renewal travel trips cannot be taken during a second renewal tour period.

38-22. EDUCATIONAL TRAVEL

a. Authority and eligibility requirements for travel and educational allowances of student dependents of civilian employees in foreign areas and Panama for the purpose of attending school are contained in the DSSR. Dependent educational travel is authorized for two types of education: secondary (grades 9 through 12) and college (academic courses leading to a degree).

b. Educational travel will be authorized for secondary education only when the nearest secondary DoD-operated school (or school approved by the DoD as a tuition/fee school under contract when no local DoD school is available) is so far distant for daily commuting from the employee's permanent duty station that room and board is needed to attend.

c. The first educational trip must originate outside of the United States. Subsequent round trips may originate at the overseas post or in CONUS. Travel expenses to a school in the United States from the employee's post and return, one round trip per year, are allowed. The next round trip may not commence earlier than one year from the date that the first round trip commenced. Under no circumstances may a dependent be authorized more than one round trip per year. A separate set of orders will be prepared by Code 10A for each half of the round trip travel.

d. In order to be eligible for secondary education travel, a dependent must not have reached his/her 21st birthday. College educational travel is restricted to those dependents who have not reached their 23rd birthday.

38-23. PASSPORT REQUIREMENTS

a. All special agents are required to maintain valid official passports. Upon notification of transfer to an area requiring a passport, the agent should immediately obtain no-fee official passport applications for each dependent who will accompany the agent to the foreign area.

b. Agents assigned to NCISHQ or to the DC Field Office should contact NCISHQ Code 10A for assistance with official passports. All other agents should contact their respective servicing Personnel Support Detachment (PSD). Applications should be presented for

processing well in advance of transfer dates since average completion time for official passports is 4-6 weeks.

c. Two photographs and proof of birth must be presented for each applicant. Acceptable proof of birth can be the original birth certificate or a previously issued passport.

d. NCISHQ Code 10A or the PSD will provide the traveler with information regarding which countries require a visa. The visa should be requested at the time the passport applications are submitted.

e. Passports will be issued with all required visas, are valid for 5 years from the date of issue, and are for official travel only. Employees and dependents desiring to perform tourist travel while assigned overseas should also obtain a regular tourist passport at their own expense.

38-24. SEPARATE MAINTENANCE ALLOWANCE

a. Separate Maintenance Allowance (SMA) is intended to assist an employee assigned to a foreign duty post offset the additional expenses incurred when he/she must maintain a separate household for dependents elsewhere. Conditions compelling this requirement may include dangerous living conditions, notably unhealthful conditions or excessively adverse conditions such as climate, altitude, lack of medical facilities or chronic lack of housing at the post of duty.

b. SMA may be granted when the employee is separated or the conditions noted above appear to require a separation of at least 90 consecutive calendar days. The 90 day minimum separation requirement may be reduced to 30 days when:

(1) Adequate medical facilities in the area are not available for pre- and post-natal care;

(2) Members of family are detained in the U.S. for medical clearance; or

(3) Children must begin or complete a school year before the employee has arrived at the post or after the employee has departed or transferred to another foreign post.

c. SMA may also be authorized for the convenience of the employee because of substantial special need or hardship, such as career, health, education or family considerations for spouse, children, or other family members.

d. If SMA is authorized and paid, dependent travel will not be approved.

e. To receive SMA, the employee must submit complete details to Code 10A. If approved, SMA will be authorized on the PCS orders and will be reimbursed via a Statement of Actual Expenses, SF-1190.

38-25. SPECIAL PCS SITUATIONS

a. All NCIS special agents are covered by the Special Agent Mobility Program as a condition of employment. A limited number of employees in other job series are also covered by a separate mobility program. If NCIS recruits or requests an employee to transfer as part of its career development program, or as an agency directed placement, the move will be regarded as being in the interest of the government and, as such, PCS allowances will be paid. By contrast, an employee may actively pursue, solicit, or request a position change for personal reasons resulting in a geographic move from one permanent duty station to another. In this situation, such a transfer is considered to be primarily for the convenience or benefit of the employee or at his request and PCS allowances shall not be paid by the government.

b. When two employees married to one another are being transferred and both moves have been determined to be in the interest of the government, relocation allowances/entitlements may be applied to either, (1) each employee separately, in which instance neither employee is eligible for any allowance as a member of the immediate family; or (2) only one of the employees, in which case the other employee is eligible for allowances/entitlements solely as a member of the immediate family. As both moves are considered to be in the interest of the government, both employees are authorized, without a charge to personal leave, the allowable time for a HHT, if authorized, actual travel time and administrative leave for PCS related matters.

c. If two employees are married to one another and the transfer of only one of the employees is determined to be for the convenience of the government, cost PCS orders will be issued to the one employee. The spouse may, upon request, be assigned to the same geographic location as a personal accommodation. The spouse will be listed as a dependent on the employee's cost orders and will be eligible for allowances solely as a member of the immediate family. The spouse will be issued no cost PCS orders for the purpose of documenting the transfer to the new duty station. In this type of situation, the employee is authorized one LQA benefit for self and family. The employee issued cost orders will be authorized, without a charge to personal leave, the allowable time for a HHT, if authorized, actual travel time and administrative leave for PCS related matters. If the employee has been issued no cost orders and is covered by a mobility program, he/she will also be authorized such time without a charge to personal leave. If the employee issued no cost orders is not covered by a mobility program, any absences associated with the execution of the spouse's cost orders will be charged to annual leave or leave without pay.

d. If an employee to be transferred is married to a military member and the military member is also to be transferred, the employee will be entitled to PCS transfer expenses provided it has been determined that his/her transfer is in the interest of the government. This applies even if the military member spouse is being transferred at the same time to the same place as the employee, provided the married couple does not receive duplicate payments of PCS entitlements for the same purpose. As the employee's transfer is considered to be in the interest of the government, the employee will be authorized the allowable travel time and administrative leave for PCS related matters without a charge to personal leave. However, if the employee's transfer is authorized solely at the employee's request and as a personal accommodation to accompany the military spouse to the new duty station, costs for the employee's transfer will be as authorized by the military travel orders. The employee will be issued no cost PCS orders for the purpose of documenting the transfer. If the employee has been issued no cost orders and is covered by a

mobility program, he/she will be authorized the allowable travel time and administrative leave for PCS related matters without a charge to personal leave. If the employee issued no cost orders is not covered by a mobility program, any absences associated with the execution of the spouse's military orders will be charged to annual leave or leave without pay.

38-26. PREPARATION AND SUBMISSION OF TRAVEL CLAIMS

a. General Requirements

(1) Timely settlement of travel claims minimizes the potential loss of records, expedites reimbursement for authorized travel-related expenses, and enables NCISHQ to quickly adjust obligations on the books. Depending on the authorizations contained in the travel orders, any combination of several forms may be required to settle a claim. If adequate records have been maintained, preparation and submission of the claim(s) should be relatively simple.

(2) Copies of all Government Transportation Requests (GTR), airline tickets, lodging receipts and itemizations of tolls paid, baggage assistance charges, etc. should be attached in support of claimed expenses.

(3) If traveling by POV, special attention should be paid to daily mileage recordings and these should be included on DD Form 1351-2 in the space provided.

b. Partial settlement claims can and should be filed as soon as possible, and a completed claim submitted as soon as expense information is known. Final claims for the sale and purchase or lease termination transactions for which reimbursement is requested must not be later than 2 years after the date the employee reported for duty at the new permanent duty station. Filing of a partial travel claim is required within 15 days of completion of any phase of a PCS move for which an advance was drawn. This is particularly important if a delay is anticipated in filing the remainder of the claim. Such partial claims apply to travel, TQS expenses, expenses related to real estate transactions (buy and/or sell), and to payment of temporary lodging allowance and the foreign transfer allowance at new duty stations overseas. It may be necessary to submit several partial settlement claims in cases where real estate transactions or dependent travel are not completed concurrently with the travel of the employee.

c. Travel and Per Diem. DD Form 1351-2 should be used to claim travel and per diem expenses. When necessary, an addendum itinerary form (DD Form 1351-2c) may be used.

d. Temporary Quarters Subsistence Expense: TQSE expenses are also claimed on DD Form 1351-2.

e. Miscellaneous Expense Allowance: A claim for reimbursement of miscellaneous expenses is made using DD Form 1351-2, Block III. If the amount claimed does not exceed $500 (individual) or $1000 (individual plus dependents), enter “Miscellaneous Expenses = $500 or $1000, whichever is applicable, and no additional documentation is required. Any claim exceeding the $500/$1000 threshold must be fully supported by paid bills or other acceptable evidence. An addendum to the DD Form 1351-2 will suffice to document miscellaneous

expenses, provided receipts, paid bills, etc., are attached. Miscellaneous expenses in conjunction with a PCS move may be reimbursed up to a maximum equivalent of two weeks basic salary of the employee, limited to the maximum rate payable at the GS-13 level.

f. House-Hunting Trip Expenses: When authorized, claims for HHT expenses are filed using DD Form 1351-2. Per diem computations for a house-hunting trip are based on the standard CONUS per diem rate. Lodging receipts, airline tickets, car rental receipts, etc. should be appended to the claim.

g. Real Estate Expenses: Under certain conditions, employees may qualify for reimbursement for certain expenses incurred in the sale/purchase of homes or the early termination of a lease. Claims for reimbursement of these expenses are filed using FORM DD-1705 and require extensive documentation in the form of the settlement sheet(s) for each transaction.

h. Depending on the expenses claimed, ancillary documentation may be required. All items in DD-1705, Blocks I, II and III, must be completed for the sale and/or purchase portions. Block IV is to be completed by a designated local official (such as the Base Housing Officer or the Human Resources Officer), Regional Office Travel Budget Personnel, or other individual competent to interpret JTR, VOL II. The totals indicated on the face of DD Form 1705 must reflect the aggregations shown on the reverse side of the form. Items (1) through (6) of the reverse side can normally be completed from information extracted from the settlement sheet(s) presented to the employee at time of sale/purchase of real estate. Notable exceptions to the above statement would be expenses related to the sale of real estate that occur prior to settlement, possible expenses such as a survey fee, pest inspection and certification, and a credit reporting fee. For such expenses, copies of cancelled checks, paid bills, etc. should be appended to the claim.

i. Some expenses shown on the settlement documents are not reimbursable. Examples include escrow items such as pro rata charges for taxes, insurance, etc. relating to ownership of the property; finance charges of any kind; maintenance costs/charges associated with the property; and title insurance which exceeds the minimum requirements for mortgage financing. With respect to finance charges, special caution is in order.

j. If the sale of property includes an assessment of a pre-payment penalty, a copy of the mortgage instrument must accompany the claim and detail the conditions under which the penalty and amount of penalty are applicable.

k. "Points" are NOT reimbursable. If there is any possibility a particular charge could be construed to be a point, the employee should request a detailed written explanation.

l. Finally, with respect to real estate charges generally, the JTR, VOL II allows reimbursing for charges CUSTOMARILY paid by a seller or purchaser to the extent they do not exceed amounts CUSTOMARILY charged in the locality of the residence. Assistance in determining the REASONABLENESS of a particular charge or fee can be obtained from the local insuring office of the Department of Housing and Urban Development (HUD) in the area

concerned. That office, upon request, can furnish a current Schedule of Closing Costs (FHA Form 2496), which will show typical costs (guidelines) incurred for a local purchase or sale of a residence.

m. Once the DD Form 1705 has been completed and documentation obtained, it should be filed as an attachment to a claim form, DD Form 1351-2. Expenses for real estate are shown in Section III of the form. Do NOT attach originals of mortgage agreements, settlement sheets, etc. to the claim form. These documents will not be returned and may become separated and lost during the processing of the claim. The employee may be required to replace missing or misplaced documentation at any point during the settlement process.

38-27. TAXATION

a. Income Tax Liability

(1) When a finance officer settles a PCS claim, certain items are subject to federal taxation. Volume IV of the NAVCOMPT Manual imposes the following guidelines for such taxation:

(2) When no real estate transaction is involved and the total approved claim for TQSE and a house-hunting trip is over $1500.00, the excess is taxed at 25%.

(3) When a real estate transaction is involved and the total approved claim for TQSE, a house-hunting trip and/or purchase/sale of real estate is over $3000.00, the excess is taxed at a rate of 25%.

(4) The miscellaneous expense allowance is taxed at a rate of 25%.

(5) The Internal Revenue Service (IRS) has determined that payment for services by an agency/activity to a relocation services company on behalf of the employee is not income to the employee and is therefore not taxable.

b. Relocation Income Tax Allowance

(1) Payment of a relocation income tax (RIT) allowance is authorized by JTR, VOL II to reimburse eligible transferred employees for substantially all of the additional Federal, State, and local income taxes incurred by the employee (or the employee and spouse if a joint tax return is filed), as a result of certain travel and transportation expenses for which reimbursement or an allowance is provided by the government or furnished in kind.

(2) RIT allowances are not applicable to new appointees, employees assigned under the Government Employees Training Act, or employees returning from overseas assignments for the purpose of separation.

(3) The law limits the types of moving expenses covered by the RIT allowance. The RIT allowance covers only those expenses actually incurred or paid by the employee and which are NOT allowable as a moving expense deduction for income tax purposes.

(4) Following are the types of expenses or allowances covered by RIT:

(a) Enroute travel, including per diem and transportation expenses of the employee and dependents from the old to the new duty station

(b) Transportation, including temporary storage expenses for movement of HHG from the old to the new duty station.

(c) Travel, including per diem and transportation expenses incurred during a house hunting trip.

(d) Temporary quarters subsistence expenses (TQSE).

(e) Real estate expenses.

(f) Miscellaneous expense allowance.

(g) Payments, or portions thereof, made to relocation services.

(h) Expenses for the movement of a mobile home for use as a residence when movement is authorized instead of shipment and storage of household goods.

(5) Employees should consult their tax preparers and appropriate IRS, State and local tax authority publications for information on the taxability of moving expense reimbursements and the allowable tax deductions for moving expenses.

(6) RIT claims should be filed at the Disbursing Office of the Personnel Support Activity/Detachment servicing the employee's new duty station. The claim will require submission of a travel voucher (DD Form 1351-2), a RIT certification form (available locally), copies of all W-2's and Schedule SE (if applicable) for employee and spouse, original PCS orders, all claims filed under those orders, a copy of IRS Form 3903 http://www.irs.gov/pub/irs-pdf/f3903.pdf (Moving Expense Adjustment) for the tax year the employee reported the moving allowance received and IRS Form 4782, Employee Moving Expense Information, if one was provided by the Disbursing Office when the employee settled the PCS claim.

(7) JTR Vol II provides detailed information regarding covered expense reimbursements, Federal withholding tax rates, and the rules and procedures governing RIT calculations. You CANNOT file for RIT benefits until after you have filed your income tax returns for the year of your move. Employees should consult their local Personnel Support Activity/Detachment for assistance in preparing the RIT claim and in understanding the impact of filing both the claim and the associated income tax returns.

APPENDIX A - PCS PLANNING CHECKLIST

Extended Planning

If transferring to an area requiring passports, execute applications immediately through the current Field Office or NCIS Headquarters, as appropriate.

Plan itinerary and, if possible, discuss the itinerary with the transportation officer.

Complete travel questionnaire and fax, e-mail or GEN via NCISFO to Code 10A. Provide as much information as possible and carefully answer all applicable questions

Examine all household effects; list major ones; decide what will be sold, discarded, etc. Decide what will go into non-temporary storage and what will be shipped as part of the 1,000-pound express shipment.

Begin preparations for sale or lease of real estate (or give notice to landlord).
Ensure transferee and dependents receive necessary inoculations, if required.

Prepare inventory of HHG for insurance purposes.

Four To Six Weeks Prior To Move

Provide forwarding notice to Post Office.

Arrange with insurance agency to transfer homeowner's policies, etc.

Collect school records, credentials, etc., for dependent children.

Prepare a complete listing of unanswered questions for discussion with the transportation officer during a pre-move interview.

Ensure that the effective date of transfer is coordinated with the current office and that a Personnel Status Report (PSR) is transmitted as noted in NCIS-1, Chapter 9.

Two To Three Weeks Prior To Move

Request advance in pay/FTA

Conduct a complete and thorough check of your POV. Ensure it is equipped with emergency tools, flares, etc.

Close or transfer charge/credit accounts.

Close or transfer checking and savings accounts.

As necessary, purchase travelers' checks.

One Week Prior To Move

Give notice to local service people to discontinue service (e.g., trash removal, newspaper, etc.).

Initiate address change, update tax withholding information, and confirm the new work schedule (for timekeeping and other purposes)

Arrange to have major appliances disconnected (ideally, the day before the move will occur).

Obtain inoculations and arrange transportation for pets. Arrange for transportation of live plants. If going overseas, coordinate with transportation officer.

Prepare a list of those necessary "survival" items for both in-transit use, as well as the first day at your new residence (e.g., baby diapers, medicine, etc.)

Two To Three Days Prior To Move

Have all soiled clothing laundered.

Drain fuel from lawn mower and other machinery.

Dispose of any partially filled containers of liquid which could leak and cause damage to other belongings.

The Day Of The Move

Have HHG separated according to category (e.g., professional books, unaccompanied baggage, etc.)

Have appliances readied for shipment. Refrigerators and freezers should be defrosted, wiped dry inside and left open.

Have gas, electric and water meters read. Disconnect telephone.

Be present when movers arrive and remain until HHG are loaded.

Accompany the moving company representative during the inspection and tagging process.

Double check to ensure everything is picked up. (Don't forget the attic!)

Be sure you and the company's representative sign the inventory sheet. (Retain a copy.)

Ensure shipping documents reflect correct destination.

Within Six Months After The Move:

File PCS claim and forward copy of claim and PSD settlement paperwork to Code 10A, with copy to Code 14.

APPENDIX B - INSURANCE INFORMATION SHEET

1. Government Coverage. Loss of or damage to HHG, POV and other personal property shipped under orders, in conjunction with travel under orders or in connection with travel in performance of military duty, is reimbursable under the provisions of the Military Personnel and Civilian Employee's Claims Act of 1964 as amended (Title 32) United States Code, Section 240-243, and implementing Navy Personnel Claims Regulations (Manual of the Judge Advocate General, Chapter XXI). THE COVERAGE RESULTING FROM THIS ACT IS NOT INSURABLE. Although the coverage serves substantially the same purpose as insurance, the act and implementing regulations contain some limitations not applicable to insurance and some advantages not available through insurance. The characteristics of the coverage provided are as follows:

a. The maximum amount payable is limited to $25,000 per loss. This has the same effect as the policy limit of most insurance contracts.

b. The possession of the article claimed must be reasonable, useful or proper under the circumstances. In conjunction with this limitation, the Judge Advocate General may specify maximum amounts allowable for specific items or groups of items.

c. In addition to these specific limitations, the type and quantity of property claimed must be consistent with the requirements of the claimant considering his duties and the needs of his dependents. Insurance policies generally do not include this type of limitation.

d. Assignment to the United States of the right to recover against insurers, carriers, or other responsible parties is a prerequisite to payment of a claim. This is almost a universal requirement of personal property insurance as well.

e. Subject to the above limitations all loss or damage is reimbursable regardless of cause as long as the loss or damage occurs during transportation and is not caused in any way by the claimant or his agent. Most insurance contracts cover only certain types of loss and damage and exclude damage or loss caused by certain acts or occurrences.

f. The maximum amount payable is the value of the lost or damaged property at the time of loss or the cost of repair, whichever is less. This is also true of all insurance coverage and carrier liability.

2. Carrier Liability. If shipment is accomplished through the use of a GBL, the shipment will be released to the carrier at the minimum released value available for the type of shipment involved. The released value is an agreed maximum value per pound of the items being shipped and is established by law and by agreement between the shipper and the carrier. For example, on most interstate shipments the GBL specifies a released valuation not to exceed 60 cents per pound per item. If a 60 pound barrel of china is lost, the carrier's maximum liability is $36.00. The member may, if he chooses, specify a higher released valuation, but if he does so he must pay the additional shipping charge. Increased valuation can normally range from $1.25 per pound to the full value of the items shipped. Carrier liability for increased value shipments is not computed

on a per item basis but on a per shipment basis. If a shipment weighing 1,000 pounds is released at $1.25 per pound, for example, the carrier is liable for up to $1,250 of damage or loss regardless of the weight of the individual damaged or lost items. Unless the value of the total shipment exceeds $25,000 plus any private insurance coverage on the shipped items, the use of an increased valuation has little or no benefit to the property owner because any loss up to a total loss will be covered by other sources and the money paid for additional shipping charges will not yield additional coverage.

3. Additional Insurance. Other than the government coverage, basic carrier liability and increased valuation available from the carrier, additional coverage specifically designed to insure against loss or damage during transit is generally not available. Some household effects and automobile insurance contracts do, however, provide some transportation loss and damage coverage as a part of the basic policy. The amount of insurance carried and the extent of coverage for transportation loss should be considered in preparing for a shipment.

4. Because the Government coverage is gratuitous and is specifically for the benefit of only military personnel and civilian employees, if lost or damaged property is insured a claim must be filed against the insurer. To permit otherwise would give an insurer who has accepted a premium payment in return for insurance coverage the ultimate benefit of a law intended solely for the benefit of the property owner. Federal funds cannot be used to pay for damage which is the contractual liability of an insurer. Claims for loss or damage during shipment generally have no adverse effect on insurance rates. Prior to shipment, the terms of any insurance coverage should be discussed with a knowledgeable representative of the insurer. If other coverage is adequate, consideration may be given to canceling the policy prior to shipment. Before cancellation of a policy, however, thought should be given to important considerations such as the desirability of having the property insured up to the time it is released to the carrier or Government for shipment and if the same insurance coverage is desired at the new location of the property, the desirability of having the property insured immediately upon its receipt by the owner at its destination as well as any cost or inconvenience associated with canceling and reinstating the insurance contract. In this regard, the length of time the property is expected to spend in transportation and/or storage is an important factor. If the coverage provided by other sources is sufficient to reimburse a total loss and coverage under a present insurance policy is either not available or not desired at the destination, it would normally be advantageous to cancel the insurance prior to shipment. In every case, however, the terms of any policy should be examined and discussed with the insurer when there is any doubt regarding coverage or other policy provisions.

APPENDIX C - CHECKLIST FOR SHIPMENT OF POV

Responsibilities of the Employee

1. Contact local servicing military Transportation Office to ensure vehicle meets transportation requirements, and ascertain locally imposed deadlines.

2. Ensure that the vehicle is in safe operating condition.

3. Ensure vehicle has fitted required emission equipment. If a vehicle shipped to CONUSA without meeting requirements, it will be impounded at the first US port it enters by US Customs. The local servicing Transportation Office can assist you in what is required to meet US federal emission controls regulation, and thereby avoid costly fines and vehicle modification requirements.

4. Leave only items considered as normal vehicular tools in the vehicle, e.g., tools to make minor repairs.

5. Secure small items, such as thermos bottles, bottle warmers, car cushions and similar items in a container normally provided for vehicular tools and accessories.

6. Leave trunk, glove compartment and vehicle unlocked and turn in one complete set of keys.

7. Have sufficient nonalcoholic permanent type anti-freeze solution in vehicle to prevent freezing.

8. Have only a minimum amount of gasoline in vehicle when delivered to the loading port.

9. Clean surface and undercarriage to ensure that foreign matter does not harbor insect pests, in order to meet Department of Agriculture inspection requirements. (Inspection made by servicing Transportation Office.)

10. If necessary, cribs which are built into or accessory to the vehicle may be left in the vehicle.

Responsibilities of Personal Property Transportation Officer at the Loading Port

1. Ensure that the employee has complied with his/her responsibilities.

2. Remove items easily susceptible to loss or damage and pack in a suitable container.

3. Furnish a box for vehicular tools and accessories.

4. Conduct an inventory of the box with the employee, tally contents on DD Form 859 and give the member a copy.

5. Jointly with the employee or the employee's agent, inspect the vehicle and complete DD Form 788, to include emission controls.

6. Prepare vehicle for shipment, i.e., empty fuel tank and disconnect battery cables.

7. Provide secure storage space until vehicle is loaded aboard ship.

APPENDIX D - POV DROP OFF POINTS

U.S. PORTS FOR TRANSPORTATION OF PRIVATELY OWNED VEHICLES

The Personal Property Office, Base Transportation, will advise the Primary Port authorized for shipment of vehicles to and from the overseas area to which assigned. All vehicles shipped to Alaska are turned in at the Port of Seattle. Alternate loading and discharge ports involving excess cost to the member may be used if approved by the Port Commander. Documents required are orders, registration, power of attorney or letter of authorization if agent delivers POV.

East Coast

Military Ocean Terminal, Bayonne, N.J. 07002

Hours: 0800-1145 and 1300-1530 Monday thru Saturday. Closed New Year's, Thanksgiving, and Christmas
Day Phone: (201) 823-6611, 6612, 6613
DSN: 247-6611, 6612, 6613
Location: At the foot of 32nd Street, Bayonne NJ

Military Traffic Management Command (MTMC)/Pasha Group, Baltimore, MD

Hours: 0800-1600 hrs Monday-Friday (subject to change - call to confirm)
Day Phone: 1-800-631-5751
DSN: -0-
Location: 2501 Broening Highway
Baltimore, Maryland 21224

Navy Supply Center, GPPSO, Norfolk, VA. 23512

Hours: 0800-1600 Monday thru Friday, except holidays.
Phone: (804) 444-4505 or 4636
DSN: 564-4505 or 4636
Location: Enter Main Gate (2) Navy Base, Hampton & Taussing Blvd., Bldg. X13

South Atlantic Outport, North Charleston, S.C. 29406

Hours: 0800-1630 Monday thru Friday, except holidays.
Phone: (803) 743-5470, 5471, 5472
DSN: 794-5470, 5471, 5472
Location: So. Atlantic Outport is within the reservation of Charleston Army Depot, North Charleston, S.C.

Gulf Coast

Hours: 0800-1200 and 1300-1630 Monday thru Friday except holidays.
Phone: (504) 948-1197/1218
DSN: 363-1197 or 1218
Location: Gulf Outport, Bldg 601, 4400 Dauphine St., New Orleans, LA

West Coast

Military Ocean Terminal, Bay Area, Oakland, CA

Hours: 0800-1530 Monday thru Friday.
Phone: (415) 466-3365, 3366, 3367
DSN: 859-3365, 3366, 3367
Location: Bldg. S-4, Oakland Army Base, Oakland, CA.

Pacific Northwest Outport, Seattle, WA 98134

Hours: 0800-1600 Monday thru Friday, 0900-1130 Saturdays.
Phone: (206) 762-9200
DSN: None
Location: C St., SW, GSA, Region 10 Facility, Auburn, WA

Southern California Outport, San Pedro, CA. 90731

Hours: 0800-1600 Monday thru Friday, except holidays.
Phone: (213) 548-5971
DSN: 833-1639
Location: Berth 55, Outer Harbor, San Pedro.

APPENDIX E – TRAVELING WITH PETS

Many OCONUS locations have specific rules governing travelling with and importing of pets, including periods of quarantine and minimum health requirements. The following links are provided as a resource in preparing for travel with your pets.

General Info:	http://www.state.gov/m/fsi/tc/1870.htm
Hawaii:	http://www.hawaiianair.com/cargo/pets/regulations.asp http://www.hawaiiag.org/hdoa/ai_aqs_info.htm
UK:	http://www.defra.gov.uk/animalh/quarantine/index.htm

APPENDIX (F) – POLICY DOCUMENT 11-24 ADMINISTRATIVE (RENTAL PROPERTY MANAGEMENT PROGRAM)

256583 11:56 20111202 IN:SSDEMAIL #60471 OUT:NCISWWSSD #263

GENERAL ADMINISTRATION 02DEC11

FROM: 0000 GEN: 11C-0041

TO: DIST

SUBJ: NCIS POLICY DOCUMENT NO: 11-24: ADMINISTRATIVE (RENTAL PROPERTY MANAGEMENT PROGRAM)

REFERENCES

(A) NCIS-1, Chapter 38, Permanent Change of Station/Dec06
(B) JTR Volume 2, Chapter 5, Part Q, Relocation Services/ 1Aug11

1. The purpose of this policy Gen Admin is to update reference (a), Section 38-17, which sets forth the Rental Property Management Program policy for NCIS employees covered by a formal mobility agreement. Reference (b) sets forth the DoD requirements for reimbursement of costs associated with property management services.

2. This revision to the NCIS Property Management Program eliminates the option to use Defense National Relocation Program (DNRP) for property management and establishes direct reimbursement as the sole means of paying for rental property management services. Employees already enrolled in the DNRP Property Management Program are not affected by this change.

3. Reference (a), Section 38-17 is modified to read as follows:

38-17. PROPERTY MANAGEMENT PROGRAM

a. An employee covered by a formal mobility agreement or a transportation agreement who is transferred to a new permanent dutystation (PDS) and who is eligible to sell a permanent residence at the old duty station at government expense may be eligible for direct reimbursement of costs associated with property management (PM) services. Reimbursement for PM services assists in offsetting costs associated with retaining a residence at the old PDS. Reimbursement is based on the actual cost of expenses and is limited to a maximum of 10 percent of the amount of lease. The employee and/or a member of the employee's immediate family must hold title to the residence.

4. This policy will be incorporated into the next revision of NCIS-1, Chapter 38 Permanent Change of Station.

5. Questions regarding this revision can be directed t (b)(7)(E) @navy.mil.

DISTRIBUTION:
NCISHQ: ALL Department and Directorates
INFO: WWSSD/AFLT

FOR OFFICIAL USE ONLY
PAGE 1 LAST (b)(7)(E)

APPENDIX (G) - NCIS POLICY DOCUMENT NO: 16-01: ADMINISTRATIVE (PCS TRAVEL)

GENERAL ADMINISTRATION 11 JAN 16

FROM: 0000 GEN: 11C-0003
TO: DIST

SUBJ: NCIS POLICY DOCUMENT NO: 16-01: ADMINISTRATIVE (PCS TRAVEL)

REFERENCE
(a) NCIS-1, Chapter 38, Permanent Change of Station/Dec06

1. This Gen Admin announces changes to reference (a).

2. All sections of reference (a): Please note that the time limit for executing all PCS associated travel, transportation, and household good shipments is one year from the transfer date. The only PCS related entitlement or allowance that may be extended one additional year (to a maximum of two years from the transfer date), under very narrow circumstances considered to be in the Government's interest, is authorized real estate expenses.

3. Section 38-5 b. is modified as follows:

Add paragraph (6): The NCIS Travel Manager or her/his authorized appointee will sign all Transportation Agreements (DD Forms 1617 and 1618). Transportation Agreements must be properly completed and signed by the employee and NCIS Travel Manager or his/her appointee before PCS travel orders may be authorized and issued.

4. Section 38-26 is modified as follows:

Add paragraph n.: Travel section personnel in conjunction with Comptroller office personnel will perform periodic reviews of travel documents (orders, transportation agreements, and vouchers) to ensure compliance with the DON Manager's Internal Control Program. This review is to ensure proper documentation of orders, transportation agreements, correct reimbursement rates are utilized, and all claims are supported with appropriate documentation. Additionally, Comptroller office personnel will periodically review personal properly shipment payments to ensure erroneous payments are minimized.

5. These changes will be incorporated into the next revision of reference (a). The POC is Code 00F1, b6 at b6 or email shay.brunderman@ncis.navy.mil.

DISTRIBUTION
NCISHQ: ALL DEPARTMENTS AND DIRECTORATES
INFO: WWSSD/AFLT
FOR OFFICIAL USE ONLY

CHAPTER 39
TITLE: RETURN RIGHTS FOR ADMINISTRATIVE PERSONNEL ASSIGNED TO AN OVERSEAS DUTY STATION
POC: CODE 10A
DATE: JUN 08

39-1. INTRODUCTION

This Chapter establishes the Naval Criminal Investigative Service (NCIS) policy and procedure for providing return rights to administrative personnel selected from a CONUS duty station for a tour of duty at an overseas location. This policy complies with the Department of Defense (DoD) Program for the Stability of Civilian Employment, commonly referred to as the Priority Placement Program (PPP).

39-2. BACKGROUND

Special agents and other limited employees of NCIS are covered by a mobility program which requires periodic transfer between CONUS, OCONUS, and overseas duty stations. Among other provisions, the mobility program ensures continued employment of covered employees as they move from one assignment to the next. The mobility program does not cover administrative employees. Employment stability for employees not included in a mobility program, is limited to circumstances covered in DoD PPP Operations Manual, Chapter 1, paragraph D.

39-3. POLICY

a. Administrative personnel employed by NCIS at a CONUS location, who accept an assignment to an overseas duty station, are entitled to return to their position at the end of the overseas tour. The CONUS position, referred to as the permanent position, remains obligated to the employee for the duration of their overseas assignment, including any authorized extensions, up to a maximum of 5 years. In rare circumstances, return rights may be extended beyond 5 years at the discretion of the agency. Return rights are limited to the grade level of the permanent position. Grade increases that may have been achieved as a result of the overseas assignment are not included in this entitlement. Every attempt will be made to protect returning employees' pay through placement at a higher step of the permanent grade, but saved pay beyond step 10 of the lower grade will not be offered.

b. Positions encumbered by NCIS administrative personnel serving at overseas locations may be advertised for backfill, but must be identified as encumbered positions. Every effort will be made to identify placement opportunities for employees occupying encumbered positions when the overseas employee returns.

CHAPTER 40
TITLE: SUPERVISORY INTELLIGENCE SPECIALIST RECRUITMENT, EVALUATION AND SELECTION PROCESS
POC: CODE 25
DATE: MAR 08

40-1. PURPOSE

The following standard operating procedure will be used to recruit and select candidates for NCIS Supervisory Intelligence Specialists (SIS), GG-0132-13. SIS vacancies will be filled through a competitive process, without regard to race, color, religion, sex, national origin, age, marital status, or non-disqualifying physical or mental handicap. All actions will be based solely on job-related criteria and not on favoritism, personal relations, nepotism, or patronage.

40.2 PRE-RECRUITMENT PROCESS

When a SIS vacancy occurs or is anticipated, the Directorate of Intelligence (DI), NCIS Code 25, will submit a written request for recruitment action via e-mail to the Personnel Operations and Services Directorate, NCIS Code 10A. The request for recruitment action must contain a copy of the position description and a Recruitment Worksheet (Appendix (1)). Upon receipt of the required documentation, NCIS Code 10A will begin the merit staffing process.

40-3. MERIT STAFFING PROCESS

40-3.1. Announcing Vacancies

a. Internal. NCIS Code 10A will issue internal SIS vacancy announcements via e-mail. The minimum area of consideration will be NCIS-wide, limited to qualified current and previous GG-13 Intelligence Specialists and those individuals who have one year of qualifying experience at the GG-12 level by the closing date indicated in the announcement. Candidates must submit a Bid Memorandum (Appendix (2)), endorsed by their Deputy Assistant Director (DAD) or Special Agent in Charge (SAC). When the vacancy announcement closes, NCIS Code 10A will

review applications to determine basic eligibility and issue a selection certificate to NCIS Code 25.

b. External. The Assistant Director, NCIS Code 25 has the discretion of requesting an external announcement in lieu of an internal announcement. In this event, NCIS Code 10A will submit a request to recruit to the Department of the Navy's Human Resources Service Center Northwest (HRSCNW). HRSCNW will issue the vacancy announcement, accept applications, conduct a screening of candidate qualifications, and return a selection certificate to NCIS Code 10A. Current NCIS employees are eligible to apply for vacancies announced under this external process. NCIS Code 10A will forward the selection certificate to NCIS Code 25.

40-3.2. Internal Paper Rating and Ranking Board

a. A Paper Rating and Ranking Board (Board) will be convened to rate and rank candidates.

b. The Board composition will consist of:

(1) Three to five members at the grade/rank level equal to or greater than the position being filled. The chairperson will be minimally at the Assistant Director level.

(2) Civilian or military members as long as the number of military members does not exceed civilian members; and

(3) At least one minority or female member to the extent possible.

(4) The NCIS Diversity Officer or designee.

Note: A NCIS Code 10A representative may serve as the technical human resources advisor.

40-4.3. Internal Paper Rating and Ranking Procedures

a. During the paper rating and ranking process, each Board member will receive the following information:

(1) Vacancy Announcement

(a) Internal Screening Plan

(b) Rating and Ranking Panel Guidelines

(c) Applicant Documents

1. PARS for most recent cycle

2. Bid Memo

3. Resume

4. SAC/DAD Endorsement

(d) Evaluation Forms

(2) Board members will evaluate each candidate's application using the SIS Internal Screening Plan (Appendix (3)). Board members will individually assign a point value to each critical element (e.g., 5 – Outstanding, 3 – Satisfactory, etc.) based on their assessment of the candidate's successful supervisory experience/exposure; analytical competency; education and training; diversity in assignments, and strength of performance, as described in the application. Specific comments can be made in the space provided on the Internal Screening Plan Form to support the assigned rating for each element. A proctor will annotate the scores of each candidate on the Consolidated Rating Sheet for SIS Positions (Appendix (4)). Board members must sign each Internal Screening Plan and Evaluation Form.

(3) When each Board member has rated all candidates, the individual scores will be presented to the members. If there is more than a one point difference between board member ratings on any one element, the members must resolve the discrepancy before finalizing the scoring process. If such differences cannot be resolved after discussion, the scoring variance must be fully documented on the evaluation forms by the Board member(s) in question.

(4) Upon conclusion of deliberations, the proctor will annotate the composite score for each candidate on the Composite Rating Sheet for SIS Positions (Appendix (5)). The Board will examine the scores to determine the cut off point for those candidates who will progress to the interview board.

(5) In identifying a natural breaking point, consideration should be given to the number of vacancies, the total number of candidates, and the range of scores.

(6) After identifying a breaking point, a Candidate Transmittal Sheet for SIS Positions (Appendix (6)) will be prepared that contains the names of the candidates referred for interview.

40-4.4. Interview Procedures

a. An Interview Board will be convened to conduct interviews. The Interview Board may consist of the same members as the Paper Rating and Ranking Board.

b. Interview questions will be job related and objective. Interview questions must be submitted to NCIS Code 10A for the merit staffing case file.

c. Interview schedules will be established by NCIS Code 25.

d. During the interview process, board members will evaluate each candidate, and individually assign a point value to each competency (e.g., 3 – Excellent, 2 – Good, 1 - Fair) based on their assessment of the candidate's reply to the interview questions and annotate the

score on the candidate's individual SIS Board Questionnaire Oral Board Summary (Appendix (7)). Specific comments can be made in the space provided on the evaluation form to support the assigned rating for each element.

e. At the conclusion of the interviews, a proctor will annotate the individual scores on the Consolidated Rating Sheet for SIS Positions (Appendix (4)). If there is more than a one point difference between board member ratings on any one element, the members must resolve the discrepancy before finalizing the scoring process. If such differences cannot be resolved after discussion, the scoring variance must be fully documented on the evaluation forms by the Board member(s) in question.

f. Upon conclusion of deliberations, the proctor will annotate the composite score for each candidate on the Composite Rating Sheet for SIS Positions (Appendix (5)). The proctor will record the combined score for each candidate (rating and ranking score plus interview score) on the Combined Composite Rating Sheet for SIS Positions (Appendix (8)). The board members will examine the scores to determine the cut off point for "best qualified" candidates. Only the "best qualified" candidates will be certified for selection.

g. Once certified, the Inspector General, NCIS Code 00I will screen each name on the "best qualified" list to identify any relevant disciplinary action or information contained in internal investigative reports that may bear upon the employee's ability to perform effectively in an SIS position. The selecting official will weigh the employee's qualifications together with the information provided by NCIS 00I in making a final selection decision.

h. External Interview Procedures

(1) DI Program Management will review all candidate applications listed on the selection certificate, and will select those candidates whose skill sets best meet current DI requirements, for interview.

(2) Interview questions will be intelligence, Intelligence Community, and leadership focused. Interview questions must be submitted to NCIS Code 10A for the merit staffing case file.

(3) The Interview Panel will consist of:

(a) Three to five members at the grade/rank level equal to or greater than the position being filled. The chairperson will be minimally at the Assistant Director level.

(b) Civilian or military members as long as the number of military members does not exceed civilian members; and

(c) At least one minority or female member to the extent possible.

Note: An NCIS Code 10A representative may serve as technical human resources advisor.

(4) Upon conclusion of the interviews, the interview panel will make selection recommendations to the selecting official.

40-4.5. Selections

a. The Assistant Director, NCIS Code 25 will be the selecting official.

b. The selecting official will annotate, sign and date the Candidate Transmittal and return the package to NCIS Code 10A for processing.

c. NCIS Code 10A will close-out the merit staffing case file, and, for external recruitments, return the selection certificate to HRSC NW.

d. Once the selections have been finalized, they will be announced via GenAdmin by NCIS Code 25.

e. The Board Chairperson will provide feedback to non-selected candidates.

f. All selection process notes will be forwarded to NCIS Code 10 for retention.

Appendix (1) Recruitment Worksheet

RECRUITMENT WORKSHEET

Position ID	Supervisory Intelligence Specialist, GG-132-13

Position Location	

Billet Sequence Code (BSC)	

Area of Consideration:	

[Internal (NCIS Only)or External (NCIS plus other eligible candidates)]

Funded PCS Available?	YES_____ NO_____

Vice:(Name of previous incumbent)	

Special Instructions or Remarks:

1. For internal vacancy announcements only, NCIS candidates must submit a resume and bid memorandum endorsed by their SAC/DAD.

2.

Selecting Official	

Point of Contact: [Name/Phone No.]	

Appendix (2) Bid Memorandum

BID MEMORANDUM

Date:

From: Your Name, Grade, Office Code
To: Name (Bid POC listed on announcement GEN), Office Code

Subj: Gen Number/Date/Subject Title

1. Interest:

2. NCIS Background:

3. Training and Experience:

4. Additional Comments:

Sincerely,

Your Name

Copy to:
SAC/DAD _____, Office Code
Additional supervisors (encouraged, but not required)

Appendix (3) SIS Internal Screening Plan

SIS Internal Screening Plan

SIS Candidate: _____ Office: _____

Performance and Assignment History (Value Total – 25 Points) **Point Total: _____**
Mark all applicable categories.

- ☐ HQ OPS CODE TOUR (1 Point)
- ☐ HQ GEO DIV TOUR (1 Point)
- ☐ LNO TOUR (1 Point)
- ☐ FIELD TOUR (1 Point)
- ☐ RFF DEPLOYMENT (1 Point)

☐ **SUPERVISORY EXPERIENCE/EXPOSURE (5 Points)**
Candidate has served successful extended acting supervisory/squad leader/team leader/leadership experience.

☐ **ANALYTICAL COMPETENCY (5 Points)**
Candidate is highly rated for quality of analytical products or analytical impact to operations/investigations. Candidate also provides accurate judgments and assessments, and has demonstrated a proclivity for initiative efforts.

☐ **EDUCATION & TRAINING (5 Points)**
Candidate has demonstrated professional growth through continuing advanced education and training, which has resulted in an increase in expertise and responsibility, and an overall understanding of mission goals.

☐ **STRENGTH OF PERFORMANCE RATINGS (5 Points)**
Candidate is consistently and strongly recommended for supervisory positions/opportunities and performance is consistently solid; ratings reflect numerous instances of excellence in performance.

COMMENTS:

Rater _____ Date _____

001000

Appendix (4) Consolidated Rating Sheet for SIS Positions

CONSOLIDATED RATING SHEET
FOR SIS POSITIONS

CANDIDATE'S NAME: *PAPER RATING* *INTERVIEW RATING*

POSITION TITLE:

ANNOUNCEMENT #:

TECHNICAL ELEMENTS

	1	2	3	4	5	6
BOARD MEMBER						
BOARD MEMBER						
BOARD MEMBER						
BOARD MEMBER						
BOARD MEMBER (CHAIRPERSON)						
ELEMENT RATING TOTALS						

(TRANSFER ELEMENT RATING TOTALS TO THE COMPOSITE RATING SHEET FOR SIS POSITIONS)

001001

Appendix (5) Composite Rating Sheet for SIS Positions

COMPOSITE RATING SHEET FOR SIS POSITIONS

POSITION TITLE: *PAPER RATING* *INTERVIEW RATING*

ANNOUNCEMENT #:

TECHNICAL ELEMENTS

CANDIDATES NAME	**1**	**2**	**3**	**4**	**5**	**6**	**TOTAL**

(TRANSFER SCORES FROM CONSOLIDATED RATING SHEET FOR SIS POSITIONS)

001002

Appendix (6) Candidate Transmittal Sheet for SIS Positions

CANDIDATE TRANSMITTAL SHEET FOR SIS POSITIONS

POSITION TITLE:

ANNOUNCEMENT #:

CANDIDATE NAMES	TOTAL SCORE

(TRANSFER TOTAL SCORES FROM COMBINED COMPOSITE RATING SHEET FOR SIS POSITIONS)

Appendix (7): SIS Board Questionnaire Oral Board Summary

SIS Board Questionnaire
Oral Board Summary

Section A **Board Information**

Date: _____ Place: _____ Rater: _____

Section B **Candidate Information**

Candidate Name: _____
Social Security Number: _____

Section C **Scores**

Procedural Knowledge	_____
Managing People	_____
Management Questions	_____
NCIS Vision	_____
Total	_____

Section D Rater Comments

Appendix (8) Combined Composite Rating Sheet for SIS Positions

COMBINED COMPOSITE RATING SHEET FOR SIS POSITIONS

POSITION TITLE:

ANNOUNCEMENT #:

CANDIDATES NAMES	Paper Rating	Interview Rating	Total

NCIS-1, CHAPTER 41
ACQUISITION AND CONTRACTING PROCEDURES
EFFECTIVE DATE: OCTOBER 2015

TABLE OF CONTENTS **PAGE**

References:
(a) Federal Acquisition Regulation (FAR), December 2014
(b) Defense Federal Acquisition Regulation (DFAR), December 2014

41-1. Purpose. In accordance with the references, this chapter establishes policies and procedures for acquisition processes applicable to all NCIS personnel and contractors. Additional resources are posted on the Acquisition Division page on Lighthouse. If you need more assistance or have specific questions, contact the Acquisition Division directly at (b)(7)(E) @ncis.navy.mil.

41-2. Policy. NCIS will follow the policy and guidelines of the Navy Marine Corps Acquisition Regulation Supplement (NMCARS), Defense Federal Acquisition Regulation (DFARS) and Federal Acquisition Regulation (FAR). The following appendices are provided for specific guidance and information.

a. See Appendix A for common terms used in the acquisition and contracting processes.

b. See Appendix B for planning for service and supply acquisitions, the do's and don'ts of market research, and competition, which is required for all Simplified Acquisition Procedures (SAP) requests above the micro-purchase threshold ($3,500 for supplies and $2,500 for services).

c. See Appendix C for information on PR Builder, the web-based procurement system for creating purchase request (PRs), and Procurement Administrative Lead Time (PALT).

d. See Appendix D for required information to order services and supplies.

e. See Appendix E for the roles and responsibilities of a Contracting Officer's Representative (COR), including guidance on No Cost Vendor Agreements.

f. See Appendix F for handling an unauthorized commitment (UNCOM).

41-3. Cancellation. NCIS-1, Chapter 41 Acquisition Procedures, July 2014.

41-4. Chapter Sponsor. Acquisition and Logistics Department, Code 11B.

41-5. Contracting Authority.

a. NCIS. Receives its contracting warrant authority from Naval Supply Systems Command (NAVSUP). NCIS' contracting officers (KOs) have the authority to issue contracts, purchase orders, and blanket purchase agreements (BPAs) for supplies and services not to exceed the Simplified Acquisition Threshold (SAT) of $150,000. BPAs written against Federal Supply Schedules may be issued for up to $500,000. KOs may place orders up to $500,000 against fixed price indefinite delivery type contracts. KOs may also issue contract actions up to $6M for vehicle leasing and repairs. KOs may bind the Government only to the extent of the authority delegated to them.

b. Fleet Logistic Centers (FLC). Contract negotiations, awards, and administration are done by NAVSUP FLC Philadelphia and Mechanicsburg activities when supplies and services are above the stated thresholds (other than OCONUS vehicles and construction above $2,000). The Acquisition Division will process paperwork submitted by the customer and forward to FLC.

c. Naval Facilities Engineering Command (NAVFAC). NAVFAV negotiates, awards, and administers OCONUS vehicles and construction above $2,000. NCIS Acquisition Division will process paperwork submitted by the customer and forward to NAVFAC.

d. Intelligence Related Contracting Coordination Office, a division of Naval Engineering Logistics Office (NELO). Any requirements that contain or might contain sensitive or classified information at the TS/SCI level must be reviewed by the Intelligence Related Contracting Coordination Office (IRCCO). All requirements that will require a Contract Security Classification Specification DD Form 254 must be reviewed by IRCCO for determining which acquisition office will award and monitor the contract. All potential IRCCO requirements must be sent to the Security Office to review the DD Form 254. The Acquisition Division will process paperwork submitted by the customer and forward to IRCCO.

APPENDIX A
DEFINITIONS

1. Acquisition. The acquiring by contract, purchase order, or delivery/task order of supplies or services for the use of the Federal Government through purchase or lease whether the supplies or services are already in existence or must be created.

2. Acquisition Planning. The process by which the efforts of all personnel responsible for an acquisition are coordinated and integrated through a comprehensive plan for fulfilling the agency's need in a timely manner and at a reasonable cost. It includes developing the overall strategy for managing the acquisition.

3. Brand name. A purchase description or specification that calls for a particular product or feature of a product that is peculiar to one manufacturer and does not permit the offer or delivery of an equal.

4. Commercial and Government Entity (CAGE) code. A five-digit contractor identifier number assigned by the Defense Logistics Information Service to suppliers doing business with the DoD. CAGE codes provide a standardized method of identifying a given facility at a specific location.

5. Commercial item. Encompasses items that have been offered for sale to the general public but not yet sold; items that have been sold but not in "substantial" quantities; items requiring modifications customary in the marketplace or minor modifications unique to the Government; many services; and certain non-developmental items.

6. Competition. An acquisition strategy whereby more than one contractor is sought to bid on a service or function; the winner is selected based on criteria established by the activity for which the work is to be performed. The law and DoD policy require maximum competition, to the extent possible, throughout the acquisition cycle.

7. Contract. A mutually binding legal relationship obligating the seller to furnish the supplies or services and the buyer to pay for them. It includes all types of commitments that obligate the Government to an expenditure of appropriated funds and that, except as otherwise authorized, are in writing.

8. Contracting Officer (KO). A person with the authority to enter into, administer, and/or terminate contracts and make related determinations and findings.

9. Delivery order. An order for supplies placed against an established contract or with government sources.

10. Federal Supply Schedules (FSS). General Services Administration (GSA) program that provides Government agencies (and some cost-reimbursement contractors) indefinite-delivery contracts with commercial firms for commonly used supplies and services. Contracting Officers order items and services by issuing delivery orders against the schedules.

APPENDIX A (CON'T)
DEFINITIONS

11. Full and open competition. All responsible sources are permitted to compete for goods and services.

12. Invoice. Contractor's bill or written request for payment under the purchase order/delivery order for supplies delivered or services performed.

13. Market research. Collecting and analyzing information about capabilities within the market to satisfy agency needs.

14. Performance Work Statement (PWS). Statement of work for performance-based acquisitions that describes the required results in clear, specific, and objective terms with measurable outcomes.

15. Purchase order. An offer by the Government to buy certain supplies or services in accordance with the terms and conditions specified in the orders.

16. Quality Assurance Surveillance Plan (QASP). Designed to define roles and responsibilities, identify the performance objectives, define the methodologies used to monitor and evaluate the contractor's performance, describe quality assurance reporting, and describe the analysis of quality assurance monitoring results.

17. Ratification. The approval of an unauthorized commitment by an official who has the authority to approve it.

18. Simplified Acquisition Procedures (SAP). The methods prescribed in FAR Part 13 for making purchases of supplies or services valued at $150,000 or less.

19. Sole source. Only one responsible source and no other supplies or services will satisfy agency requirements.

20. Statement of Objectives (SOO). Government-prepared document with the solicitation that states the overall performance objectives. It is used in solicitations when the Government intends to provide the maximum flexibility to each offer or to propose an innovative approach.

21. Statement of Work (SOW). The scope of the technical, functional, and performance characteristics of the work to be performed. It identifies essential functions to be performed, determines performance factors, including the location of the work, the units of work, the quantity of work units, and the quality and timeliness of the work units.

22. Task order. An order for services placed against an established contract or with government sources.

23. Unauthorized Commitment (UNCOM). An agreement that is not binding because the Government representative who made it lacked the authority to do so.

APPENDIX B
ACQUISITION PLANNING, MARKET RESEARCH, AND COMPETITION

1. Acquisition Planning. Each NCIS program office will perform acquisition planning and conduct market research. Planning ensures the Government meets its need in the most effective, economical, and timely manner. Acquisition planning is a joint responsibility between the customer, finance, legal (if needed), and the acquisition teams. Acquisition planning begins as soon as the customer's need is identified. It should occur well in advance of the fiscal year in which an award is necessary. The planner should review any previous plans for similar acquisition and discuss with the contracting officer.

2. Market Research - Required Sources.

a. The program office conducts market research, which involves obtaining information specific to the item or services being acquired and should include whether the Government's needs may be met by items or services that are commercially or non-commercially available.

b. The responsibility for market research also includes avoiding certain activities prohibited under Government procurement law. Generally, the purpose of Government prohibitions is to avoid providing any one firm with a competitive advantage. These reminders will help maintain procurement integrity:

(1) Never discuss potential future employment with any firm contacted for market research information.

(2) Discontinue communicating with persons in commercial organizations after obtaining market research data.

(3) Do not accept favors from persons in commercial organizations.

(4) Avoid the appearance of impropriety in communications with commercial firms.

(5) Do not share price and sensitive data of one supplier with another.

(6) Do not disclose Government strategy or circumstances associated with the need for a product or service.

(7) Do not initiate price negotiations without involving the Acquisition Division (Code 11B1) for headquarters requirements and Fleet Logistics Centers for field office requirements.

(8) Do not solicit the supplier's input or involvement in defining requirements.

(9) Do not allow the supplier to assist in writing a SOW.

APPENDIX B (CON'T)
ACQUISITION PLANNING, MARKET RESEARCH, AND COMPETITION

(10) Do not provide the contractor with a draft copy of a SOW while performing market research.

(11) Do not request pricing information if the item or service is not a commercial item or service and prices have not been published.

(12) Get Code 11B1 involved early. Send email to (b)(7)(E) @ncis.navy.mil if you have questions.

3. Competition.

a. Competition is required for all SAP requests above the micro-purchase threshold ($3,500 for supplies and $2,500 for services). A minimum of three sources are required. All SAP requirements greater than $3,500, but no more than $150,000 are reserved exclusively for competition among small business concerns and must be set aside for small businesses. If the requirement is a sole source above the micro-purchase threshold a Sole Source or Brand Name Justification form shall be completed. The form must include the following:

(1) Description of the item, to include the critical or unique requirements that are mandatory and that limits the requested item to a sole source/brand name.

(2) If the contractor has a unique expertise and /or unique equipment, explain.

(3) Ensure the supply/service to be acquired from the one source meets the requirements.

b. The following are NOT considered a justification:

(1) Statements that a contractor has the best capability or it's the only known source.

(2) Incumbency.

(3) Timeframe; if this has a major impact, explain.

(4) Similar products lack necessary features to meet Government's minimum needs.

c. For Sole Source and Brand Name Justification forms, see "Acquisition Planning Package" on Lighthouse: (b)(7)(E)

(b)(7)(E)

APPENDIX C
PR BUILDER AND PROCUREMENT ADMINISTRATIVE LEAD TIME (PALT)

1. PR Builder. PR Builder is a web-based procurement application developed by the Marine Corps. The automated purchase request (PR) process provides information on PR status at each step of the approval process, including email notification at each milestone. If there is a system-wide PR Builder application outage that lasts longer than two working days, the process for submitting a PR reverts to the NCISHQ 4238 manual system. If the original PR was submitted manually any modifications or changes should also be submitted manually through the Comptroller (Code 00F) for approval. For questions on PR Builder and PR Builder training, refer to the Lighthouse page at: (b)(7)(E) (b)(7)(E)

2. Purchase Request Package. All PR packages must include the following:

a. Authorizing signature.

b. Requisition number.

c. Three suggested sources for requirements above the micro-purchase threshold. (See Appendix B, paragraph 2, Market Research—Required Sources.)

d. Funding data.

e. Brand Name Justification or Justification for Sole Source form, as applicable.

f. Quantity and unit of issue.

g. Place of performance, delivery date, and location(s).

h. Copy of all data received from market research.

i. All IT requirements (hardware, software, cellphones, fax machines, pagers, scanners, copiers, etc.) must have Section 508 certifications and be routed to Code 15 for review and coordination, and to obtain an approved ITPR, in accordance with the DONCIO mandate.

3. Procurement Administrative Lead Time (PALT). PALT identifies the time it takes to process a PR. The PALT starts when a completed acquisition package is accepted by the Contracts Branch and ends when an award is made. PALT for end-of-fiscal year and beginning-of-fiscal year requirements are published annually. A Gen Admin provides due dates for all requirements that must be awarded by the end of the current fiscal year. All requirements must be received with accurate documentation. This includes PWS for services, SOW, and specifications for equipment, if applicable. Proper certifications, coordination/approvals, and certified funds are also needed before processing PRs. If the budget has not been approved for

APPENDIX C (CONTINUED)
PR BUILDER AND PROCUREMENT ADMINISTRATIVE LEAD TIME (PALT)

the coming fiscal year, the "Availability of Funds Clause" must be on the PR.

4. Priority Numbering System. When there is a system wide outage lasting longer than two days all PRs and 4238s must follows the priority numbering system below:

a. Priority 1: Mission critical and urgent.

b. Priority 2: Performance impaired but not critical or urgent.

c. Priority 3 to 15: Routine.

5. SACs, DADs, and/or higher authority are required to endorse Priority 1 acquisition requests. Such requests should be rare and submitted only when the requirement is both urgent and mission critical. Priority 1 requests will be processed ahead of all other requests. Priority 1 requests must be submitted separately from other requests. FO's and departments submitting more than one Priority 1 request in a one month period must obtain endorsement and written justification from the EAD/AD.

APPENDIX D
PURCHASE REQUEST PACKAGES FOR SERVICES OR SUPPLIES

1. Ordering services. PR package must include the following:

a. PWS, SOW, or SOO, as applicable.

b. Justification and Approval (J&A), as applicable, for actions over $150,000.

c. Management and Oversight Process for the Acquisition of Services, as applicable.

d. Quality Assurance Surveillance Plan (QASP), as applicable.

e. Independent Government Estimate (IGE).

f. Funding document—an approved PR or Form 2276, as applicable.

g. Manufacturer (if item is to be repaired), including:

(1) Original acquisition purchase price. If follow on or new effort with the same company, indicate model/part/serial number for each piece of equipment to be repaired.

(2) Specific description and details of the problem ("Does not work" is insufficient).

(3) Where the work is to be completed (address, floor, room number, etc.).

(4) Required completion date for the service/repair.

(5) Military specification (MIL SPEC), Federal specification (FED SPEC), technical manuals or drawings, etc., that must be met.

(6) Manufacturer's Commercial and Government Entity (CAGE) code, if known, and a complete address of manufacturer and suggested source if different from manufacturer.

2. Ordering Supplies. PR packages must have the following:

a. Funding document—an approved PR or 2276, as applicable.

b. Complete item description, to include minimum critical features that the equipment must contain, and a copy of a drawing or photo, if applicable.

c. Complete description of end item, including manufacturer, model, serial number and

APPENDIX D (CONTINUED)
PURCHASE REQUEST PACKAGES FOR SERVICES OR SUPPLIES

color, if applicable.

d. Three suggested sources for requirements above the micro-purchase threshold. (See Appendix B, paragraph 2, Market Research—Required Sources.).

e. Sole source or brand name justification (for unique requirements).

APPENDIX E
CONTRACTING OFFICER'S REPRESENTATIVE (COR)

1. Contracting Officer Representative (COR). The COR monitors the contractor's performance and serves as the technical liaison between the contractor and the contracting officer.

a. The contracting officer is responsible for the contract, including terms and conditions, and for ensuring that the contractor satisfies the requirements stated in the contract.

b. Only a duly appointed contracting officer has the authority to enter into and administer a contract on behalf of the U.S. Government, change or terminate an existing contract, and make determinations and findings relating to the contract.

c. The COR's authority is received by appointment from the contracting officer. This appointment must be made by the contracting officer in writing, clearly describe the limits of the COR's authority, and confirm that the COR has received appropriate training.

d. The COR must acknowledge receipt of the delegation letter in writing and read and understand the contractual agreement. Also, the COR must fulfill the Government's commitments to the contractor and serve as a liaison between the contracting officer and the contractor. The COR must also monitor the contractor's performance under the contract and ensure that the contractor delivers what is called for in the contract.

e. The COR and contracting officer, together, must ensure the contract calls for delivery of products and services that satisfy the bona fide needs of the Government.

f. All NCIS CORs must register for the DoD Contracting Officer Representative Tracking (CORT) Tool, a web-accessible application that allows NCIS to track COR nominations, appointments, terminations, and training certifications.

g. The COR should report any perceived unauthorized commitments immediately to the Contracting Officer. At the same time, CORs themselves must take great care not to instruct a contractor to perform a task that may be outside the scope of the contract. CORs are reminded that they, or any unwarranted Government official, may be financially obligated for any costs or damages incurred as a result of their directing contractor performance beyond the scope of their authority. If a COR exceeds his or her authority, the circumstances of the action and the procedures in FAR 1.602-3 concerning ratification will dictate what action should be taken. The Contracting Officer may decide to revoke the COR's appointment. The revocation shall be in writing and provided to the contractor and other appropriate officials. The Contracting Officer will also take other actions required by law or regulations.

h. For more information, see the "Contracting Officer's Representative" on Lighthouse.

(b)(7)(E)

APPENDIX E CONTINUED)
CONTRACTING OFFICER'S REPRESENTATIVE (COR)

2. No Cost Vendor Agreements. Only a contracting officer has the authority to enter into a No Cost Vendor Agreement on behalf of NCIS. When a commercial vendor offers NCIS the opportunity to test equipment or other products at no charge, the agreement between the vendor and the Government must be in writing. The purpose of a signed agreement between NCIS and the vendor is to ensure that NCIS is protected from liability, not obligated to purchase the item(s), and that the contractor cannot use NCIS testing as an endorsement of the item(s). Agreements are completed by the Acquisition Division and will contain the vendor's name, address and point of contact, a description of the supplies or services, and the duration of time to test. For more information and a copy of the agreement, contact the Acquisition Division at (b)(7)(E) @ncis.navy.mil.

APPENDIX F
UNAUTHORIZED COMMITMENT (UNCOM)

1. Unauthorized Commitment (UNCOM). An agreement that is not binding solely because the Government representative who made it lacked the authority to enter into that agreement. Only contracting officers acting within the scope of their authority are authorized to enter into binding agreements or make modifications thereto on behalf of the Government.

a. Only an action that would otherwise be proper can be ratified. The approving official cannot elect to use his or her discretion to reimburse the contractor or vendor for acts exceeding the employee's authority. The employee can be held personally liable for any costs or damages incurred by the contractor or the Government. In fact, the consequences for all parties involved with an unauthorized commitment are severe. Regardless of dollar amounts involved, unauthorized commitments may result in disciplinary or administrative action against the individual making the unauthorized commitment, especially if the violations are flagrant or repetitive.

b. In order for NAVSUP to make a determination with respect to ratification should an UNCOM occur NCIS must follow the below requirements:

(1) The employee who committed the UNCOM is required to gather documentation and write the Statement of Fact (SOF).

(2) Code 00F determines whether funds are available and were available at the time the UNCOM was made.

(3) Code 11B reviews all documentation.

(4) Code 11C uploads package to the Taskers system.

(5) Code 10 reviews the package to determine if disciplinary action is warranted.

(6) Code 00L reviews any documentation that requires a legal review.

(7) The NCIS Director signs the letter requesting ratification from FLC.

2. Ratification process. The employee must provide a signed SOF describing the circumstances. The UNCOM package is online at

(b)(7)(E)

a. The employee's SOF must address for following:

(1) Describe the circumstances that caused the unauthorized commitment.

(2) Why normal and correct procurement procedures were not followed.

APPENDIX F (CONTINUED)
UNAUTHORIZED COMMITMENT (UNCOM)

(3) Whether procedures existed to avoid an unauthorized commitment?

(4) The bona fide Government needs that dictated making the commitment.

(5) Whether any benefit (and its value) was received.

(6) Whether funds are available and were available at the time of the UNCOM.

(7) How and when the item or service was identified as an UNCOM.

(8) What attempts (if any) were made to resolve the UNCOM prior to requesting authorizations (such as returning merchandise) and any other pertinent facts.

b. Additional documents required to ratify the UNCOM:

(1)Contractor supporting data, including original invoices and other documents that show evidence of the transaction.

(2) Purchase description, via PR Builder or 4238, processed through Code 00F.

(3) Unauthorized Commitment training certificate.

3. Review and Payment. Code 11B reviews the request for ratification submission, provides training information on TWMS, and recommends any additional actions. Code 11B will also prepare a letter from the Director to FLC addressing the UNCOM. The letter describes measures taken to prevent a recurrence and requests FLC to ratify the UNCOM. Once the Director signs the letter, Code 11B will submit the package to FLC for processing. It may take 6-18 months before the vendor is paid.

4. Avoiding UNCOMs. The following are common ways violations occur:

a. Purchasing services and supplies without funding.

b. Assuming a PR was submitted for renewal of services and supply or service continues.

c. A contractual agreement called for maintenance of five copy machines, but the contractor performs maintenance on six machines.

d. Exceeding the dollars or hours of the purchase order/delivery order (PO/DO).

e. Someone other than the Government cardholder contacted the vendor to request supplies or services and advised that the cardholder will “call with the Visa number.”

APPENDIX F (CONTINUED)
UNAUTHORIZED COMMITMENT (UNCOM)

f. Unclear communication between the customer and vendor.

g. Contractor performs services that are not included in the PO/DO or contract.

h. Contractor delivers a supply or service that is not in the PO/DO. A Government employee accepts it and no funding is obligated on the PO/DO.

5. Best Practices

a. Maintain dialog with your acquisition team in Code 11B.

b. Comply with Federal laws. Only an employee with proper delegated procurement authority may purchase supplies or services on behalf of the Government.

c. Have an approved PR from the Comptroller's office.

d. Follow the PR process described online at (b)(7)(E) (b)(7)(E)

e. Complete all necessary steps before supplies or services are ordered.

f. Ask questions to the acquisition team before you commit.

g. Allow only persons with the appropriate authority to make purchases.

h. Verify with Code 11B that you have authority to purchase with the GPC.

CHAPTER 42
TITLE: PUBLIC AFFAIRS: MEDIA RELATIONS, CONGRESSIONAL AFFAIRS, AND LAW ENFORCEMENT LIAISON
POC: CODE 00C
DATE: SEP 08

POLICY DOCUMENT:

APPENDIX (3): Gen Admin 11C-0025 of 3 Dec 2012 released NCIS Policy Document No. 12-14: Administrative (NCIS Retirement Gen Admins). Policy Document 12-14 contains revised or new policy that has not been incorporated into this chapter and should be reviewed in its entirety.

42-1. INTRODUCTION

The mission of the Naval Criminal Investigative Service (NCIS) Communications Directorate, Code 00C, is to produce, coordinate, and distribute information about NCIS, both internally and externally. Code 00C will ensure timely and accurate dissemination of information to public, government, and media entities. This includes an active liaison program with other Department of the Navy (DON) organizations, federal government agencies, state and local law enforcement organizations, the U.S. Congress, as well as a variety of news media outlets. Code 00C also has responsibility to keep NCIS employees informed of important information that has an impact on the entire organization. This chapter will delineate responsibilities for the release of information to external sources, such as the media, the general public, and various congressional and government entities. All employees of NCIS must be familiar with the contents of this chapter. NCIS-1 Chapter 42 covers the following sections based on the departmental responsibilities of Code 00C: Public Affairs, Media Relations, Congressional Affairs, and Law Enforcement Liaison.

42-2. PUBLIC AFFAIRS

42-2.1. Public Affairs Organization. The following is a summary of where NCIS Public Affairs fits in within the Department of Defense public affairs arena.

a. Department of Defense (DoD). The Assistant Secretary of Defense for Public Affairs (ASD(PA)) is responsible for all DoD external and internal information, per DoD 5122.5. ASD(PA) coordinates the exchange of information with the service information chiefs.

b. Department of the Navy (DON). The service information chief for the Navy is the Chief of Naval Information (CHINFO) who coordinates the flow of all external information for DON, per SECNAVINST 5720.44B. CHINFO reports to and receives public affairs (PA) guidance from the ASD(PA).

c. Marine Corps Public Affairs. The service information chief for the Marine Corps is the Deputy Chief of Naval Information for Marine Corps Affairs, also known as the Director of Public Affairs (DIRPA), Headquarters Marine Corps. DIRPA coordinates all information flow for the Marine Corps, per SECNAVINST 5720.44B.

d. Command Public Affairs Officer. The Public Affairs Officer (PAO) is the principal advisor and staff assistant to the commanding officer for all public affairs matters; in essence, the "subject matter expert" for public affairs. The command level or base PAO will usually be a trained military professional; however, many commands retain civilian media specialists who possess the title of PAO. Navy and Marine Corps PAO personnel are assigned to most DON activities and should be called upon and consulted with by NCIS offices with public affairs issues. Because NCIS has no authority to issue press releases, all releases of information to the media, written or verbal, must be thoroughly coordinated with the local PAO. Special efforts should be made by all levels of NCIS leadership to routinely meet with the PAO within their area of responsibility to promote cooperative working relationships. It is recommended that designated members of the leadership team at each NCIS office liaison with their local command PAO at a frequency that will foster a cooperative working relationship and lead to a successful NCIS Public Affairs program.

e. NCIS Public Affairs. The Assistant Director of Communications is responsible for NCIS public affairs. Code 00C is the agency liaison and coordinating office for all issues involving CHINFO and DIRPA, and will assist field components in fulfilling their media responsibilities.

42-2.2. NCIS Public Affairs Office. Code 00C coordinates agency activities with all other governmental public affairs activities and is responsible for:

a. Managing the worldwide NCIS PAO Program.

b. Responding to law enforcement and other mission inquiries from the media, and keeping the appropriate higher authorities informed.

c. Monitoring national media trends and formulating a communications strategy.

d. Coordinating and monitoring all media interviews by NCIS Headquarters (NCISHQ) and field level personnel.

e. Conducting liaison with the public affairs offices of other federal, state and local law enforcement agencies and coordinating NCIS representation at national and international law enforcement and related conventions.

f. Formulating media guidelines and providing training.

g. Maintaining a news clip file on NCIS activities and events that have been submitted to the PAO by NCIS field elements.

h. Coordinating and approving the design, production and distribution of all NCIS external communication products, e.g., brochures, articles, and videos.

i. Coordinating and approving the design, production, and distribution of internal communication products, including the NCIS Bulletin, the weekly 'News to You', and videos.

j. Coordinating and approving the design and content of all unclassified NCIS websites available to the public via the Internet and available internally via the NCISnet.

k. Editing and disseminating Gen Admin documents regarding the death of NCIS employees or their immediate family members.

l. Conducting such other public affairs duties as may be required.

42-2.3. NCIS Headquarters Directorate Responsibilities. Due to the unique worldwide operational mission of NCIS and significant media interest in NCIS activities, program managers at NCISHQ and field supervisors are responsible for ensuring that Code 00C is provided with timely information on operational issues that occur throughout the organization and that may generate media interest. In addition, program managers should keep Code 00C informed of significant program changes and of events that highlight the professionalism of NCIS, so these advances can be included in agency briefings made by the public affairs staff. In their capacity as "subject matter experts", headquarters personnel may be requested to brief media representatives on mission goals, achievements, and operational issues. Any media-initiated contact with headquarters personnel must be referred to Code 00C in a manner that ensures timely public affairs coordination.

42-2.4. All NCIS employees should look for opportunities to promote NCIS' professional image. The Special Agent in Charge (SAC) and other field supervisors should keep Code 00C informed of any "proactive media endeavor" they are considering initiating and/or actual potential public affairs events that they feel can be enhanced by the support or guidance of NCIS Code 00C. All proactive media endeavors in the field must be coordinated with and approved by the local PAO and Code 00C.

42-3. MEDIA GUIDELINES

The importance of a good working relationship between NCIS, the DON public affairs community, and the news media (TV, print, radio, Internet, etc.) cannot be overstated. It is the

policy of NCIS to cooperate with authorized news media representatives in their efforts to gather factual public information pertaining to the activities of NCIS, as long as this does not interfere with investigations, infringe upon individual rights, or violate the law or standing DoD or DON instructions or guidance. Such cooperation must be fully coordinated with CHINFO and DIRPA, as appropriate.

42-3.1. The following set of guidelines for dealing with the news media (TV, print, radio, Internet, etc.) supersedes any existing or previous NCIS policy. Every contact between NCIS offices and the news media must be closely coordinated from start to finish with the cognizant Navy or Marine Corps PAO. No NCIS agent or employee has the authority to speak with, or in any way interact with, the media unless the following conditions are met:

a. Press Releases. Because NCIS does not have DoD or DON authority to issue press releases, all press releases written about matters exclusive to NCIS must be approved and disseminated by the cognizant PAO of the Navy or Marine Corps. Press releases sent by another agency with mention of NCIS with a description of our role in a case are also required to be approved by the cognizant PAO. Any such press releases must also be coordinated with Code 00C.

b. Press Conferences. Press conferences on NCIS cases must be fully approved and organized by the cognizant Navy or Marine Corps PAO. In press conferences where NCIS is a participant, the SAC, or his/her designee or representative, must coordinate every aspect of the press conference with the cognizant PAO, including what the NCIS representative will say. Any such press conferences must also be coordinated with Code 00C.

c. Media Interviews. All interviews of NCIS special agents and professional staff by members of the news media must be coordinated with and approved by the cognizant Navy or Marine Corps PAO Officer, and by Code 00C. It is essential that the PAO or a Code 00C representative be present when any interview takes place. During interviews, NCIS representatives should always be truthful, accurate, professional, and fully prepared; they must not stray outside the area of their competence or beyond what is approved by the PAO or Code 00C.

d. Media Inquiries. Unsolicited inquiries from the news media must be directed promptly to the cognizant Navy or Marine Corps PAO and to Code 00C. Any NCIS response should be closely coordinated with that PAO. Only the SAC, or his/her designee, is authorized to speak for NCIS in the field, and only when this has been fully coordinated with the PAO and Code 00C. NCIS representatives who field calls from the news media should keep in mind the deadlines that the media work under and be as prompt as possible in responding to inquiries.

e. Proactive Media Outreach. On occasion the media can be a conduit for soliciting information about an open case, for instance asking the public's assistance in providing new information about a cold case. Any such initiative should be coordinated with and approved by the cognizant Navy or Marine Corps PAO. In addition, the NCIS operational chain of command and Code 00C should be consulted and routinely informed about any proposed initiative.

42-3.2. Specific Instructions on Media Inquiries Regarding Open Cases.

Subject to the coordination requirements outlined in Section 42-3.1, there are certain types of information, detailed in addenda to this chapter as noted below, that may be released to the media in connection with investigations, arrests, and the filing of indictments. With the exception of those circumstances detailed below, the standard response to media inquiries regarding open investigations should be as follows: "In the interest of investigative objectivity, victim privacy considerations, and the rights of the accused, NCIS does not comment on its ongoing investigations."

a. For the types of information that can be released in connection with an investigation of a crime or an event, see Appendix (1).

b. For the types of information that can be released following an arrest or the filing of an indictment, see Appendix (2), attached (per Section 0142 of the JAG Manual).

c. It is recommended that the SAC of each field office, or his/her designee, visit regularly with the local Navy or Marine Corps PAO to inform them of the NCIS mission and keep them apprised of NCIS open cases that could attract media attention.

42-3.3. Media Crisis Management. In the event of a crisis, Code 00C should be notified at the earliest opportunity, at which time Code 00C Public Affairs support will be made immediately available. As a rule, the responsibility for the media on a military facility rests with the base PAO. NCIS offices should proactively engage the local PAO to ensure that joint protocols for dealing with the media in a crisis are developed, understood, and ideally, exercised in advance of an actual crisis. The onset of a crisis is the wrong time to start thinking about these issues. The local PAO should be an active participant in any NCIS-coordinated law enforcement crisis management exercise.

42-3.4. Photographs. Photographs should be taken in accordance with DoD 5040.6-M-2, Instruction for Handling Visual Information (VI) Material, 20 Apr 05. NCIS employees, contractors, or affiliated personnel should not release such material without prior notification being made to Code 00C. Generally, the only time photographs of suspects are released is when they serve a law enforcement purpose, such as requesting public assistance in locating a suspect who is wanted in connection with a crime, a victim of a crime, or a missing person in an ongoing investigation.

42-4. PUBLIC AFFAIRS ADMINISTRATIVE REQUIREMENTS

42-4.1. News Clips. Field supervisors must monitor all local/regional media for stories concerning NCIS. If the article in question is in a newspaper or magazine that can be found on-line, field supervisors should email the on-line address and article information to Code 00C in a timely manner. Original articles which mention NCIS by name and originate in publications not found on-line should be cut out of the publication, neatly posted on an 8 ½-by-11 inch white bond paper with the following information typed in the upper left hand corner of the paper:

a. Name of Publication (underlined)
b. City and State
c. Day and Date
d. Page Number

The article should then be faxed or mailed to Code 00C at NCISHQ.

42-4.2. Publishing and public speaking. NCIS employees are encouraged to promote the NCIS mission, both within and outside their work environments. This may include writing articles for publication or participating in public speaking events. All writings and public speaking engagements by NCIS employees must be in accordance with Code of Federal Regulation Title 5 C.F.R. 2635.807 and DoD 5500.7-R, Section 2-207.

a. Articles authored by employees of NCIS that are intended for external publication must be submitted to Code 00C for content, policy and security review. The purpose of this review is to ensure quality control and a consistency of NCIS policy statements made in public fora. If there is any question about the classification or security aspects of an article or speech, it will be referred to Navy Information and Personnel Security Programs Department (NCIS Code 24E) at NCISHQ for further review.

b. All public speaking engagements and appearances in which an NCIS employee is representing NCIS must be approved of at not lower than the SAC or Deputy Assistant Director (DAD) level. The SAC/DAD should seek guidance from the local PAO and from Code 00C prior to approving any such speaking appearance.

42-4.3. Access and participation in the Internet/World-Wide Web. As all facets of society, both private and governmental, seek new and broader means to communicate, it is increasingly evident that the Internet and the World-Wide Web are significant means to this end. Code 00C is the functional manager for the external Internet program and is responsible for all content on and design standards for NCIS internal and external unclassified websites. All Internet materials and World-Wide Web sites must be in compliance with the DoD Web Site Administration Policies and Procedures memo of 25 Nov 97 (updated 11 Jan 02) and SECNAVINST 5720.47A (DON Policy for Content of Publicly Accessible World Wide Web Sites).

42-5. CONGRESSIONAL AFFAIRS

42-5.1. Background. Code 00C oversees all communication with the U.S. Congress, including those communications that take place in the field at the request of congressional members (senator or representative) or other national leaders. When such conversations with congressional members or other national leaders occur in the field, Code 00C must be notified in a timely manner. Code 00C also coordinates and expedites NCIS responses to congressional inquiries, and coordinates with DoD, DON, and other federal agency legislative affairs offices on issues affecting the employees and mission of NCIS. Moreover, Code 00C tracks legislative proposals with the potential to affect NCIS employees and the NCIS mission. Code 00C is also responsible for managing the NCIS Legislative Fellowship (Legis Fellow) Program.

42-5.2. Congressional Affairs Organization. Given its critical importance to DON and, more broadly, DoD success, the Congressional Affairs portfolio is carefully managed by DoD and DON senior officials. Code 00C has responsibility for ensuring that NCIS congressional liaison activities are coordinated with and supportive of these senior officials. It is imperative that NCIS program managers and field supervisors report any substantive contact they have with congressional members (senator, representative, or staff) to Code 00C promptly. This will enable Code 00C to assure that appropriate coordination can be effected with DoD and DON seniors responsible for Congressional Affairs, and that NCIS equities will be properly addressed. The following are key officials in the DoD/DON Congressional Affairs apparatus:

a. The Assistant Secretary of Defense (Legislative Affairs) is the principal staff advisor to the Secretary of Defense and Deputy Secretary of Defense for DoD relations with members of congress (senators and representatives) per DoD Directive 5142.1.

b. Within the DON, the Chief of Legislative Affairs (CLA) is the Secretary of the Navy's principal staff assistant for discharging the legislative functions and responsibilities of the DON, with the exception of liaison with the Appropriations Committees, per SECNAVINST 5730.5H. The CLA heads the Office of Legislative Affairs (OLA).

c. The Chief of Legislative Affairs is aided by a Deputy Chief of Legislative Affairs for Marine Corps Matters (DCLA(MC)), who shall serve as the principal assistant to CLA for Marine Corps matters. Per SECNAVINST 5730.5H, the DCLA(MC), also known as the Legislative Assistant to the Commandant, may report directly to the Secretary of the Navy regarding matters solely related to the Marine Corps. The DCLA(MC) heads the Marine Corps Office of Legislative Affairs.

d. Congress has directed that a separate and independent organization within the DON conduct liaison with the Appropriations Committees. SECNAVINST 5730.5J establishes that the Assistant Secretary of the Navy for Financial Management and Comptroller (ASN(FM&C)) is responsible for the DON's relations with these committees and all related DON appropriations matters. Within ASN(FM&C), the Director of the Appropriations Matters Office (FMBE) is specifically assigned responsibility for all appropriations-related functions.

42-5.3. NCIS Congressional Affairs Responsibilities. Responsive, accurate, and professional interaction with congressional members (senators, representatives, and their staffs) is crucial to effective congressional oversight, the organizational reputation of NCIS, and, ultimately, NCIS mission accomplishment. Assisting in the prompt response to congressional inquiries is a responsibility of all NCIS employees. Prompt, effective and, above all, accurate communication with Congress requires a team effort by all employees responsible for the programs and activities of interest to Congress. Code 00C is responsible for coordinating this team effort and all interaction with Congress.

a. In keeping with these requirements, Code 00C is responsible for:

(1) Coordinating with the Navy Office of Legislative Affairs (OLA), the Marine Corps Office of Legislative Affairs, the ASN(FM) Appropriations Matters Office, and other DoD and

federal legislative liaison offices on all matters relating to legislation, congressional oversight, and all other congressional areas of interest and related liaison requirements and responsibilities.

(2) Coordinating with NCIS program managers, field supervisors, and other executives on all NCIS responses to congressional inquiries regarding completed and ongoing NCIS investigations and operations, programs, policies, systems, administrative and employee matters, and other concerns.

(3) Coordinating with NCIS program managers and relevant DoD, DON, and other federal officials on all matters involving NCIS budget justification for Congress or congressional inquiries regarding budget execution.

(4) Coordinating preparation of NCIS officials called to testify before or brief congressional members, staff, or committees.

(5) Responding to inquiries from NCIS personnel regarding proposed legislation that could affect the mission or personnel of NCIS.

(6) Coordinating all official NCIS liaison activities with members of Congress, congressional committees, and congressional staff.

b. Headquarters Directorate Responsibilities. Headquarters staff and field supervisors are responsible for providing Code 00C with timely and accurate input for NCIS responses to Congress. This input may include investigative summaries and statistics. Headquarters staff may be required to brief congressional members (senators, representatives and/or their staff) or testify before Congress on NCIS investigations, operations, programs, plans, and policies. Code 00C will coordinate congressional briefings and prepare testimony.

c. Field Office Responsibilities.

(1) On occasion, members of congress (senators, representatives, or their staff) initiate direct communication with NCIS field personnel. Often, these contacts deal with ongoing investigations; complaints by constituents regarding NCIS investigations, investigators, investigative techniques and policies; joint operations involving other naval, DoD, or inter-agency elements, or the like. When congressional inquiries touch on these or other potentially sensitive areas, they should be promptly referred to NCIS Code 00C. The field office SAC has responsibility for promptly notifying Code 00C of any direct inquiries from:

(a) Members of Congress (senators and representatives); and/or,

(b) Congressional staff; and/or

(c) Congressional committees.

(2) SACs are also responsible for promptly notifying NCIS Code 00C of requests from supported commands, Navy or Marine Corps OLA, Navy JAG, Marine Corps SJA, or the Naval Inspector General for NCIS input to command replies to congressional inquiries.

(3) If a direct inquiry from Congress on any investigative issue or topic that can be construed as sensitive is received in the field, the SAC should:

(a) Ascertain the nature of the inquiry, specific information desired, name and telephone number of the constituent (if relevant), name and telephone number of the congressional member (to include staff), any deadline, and information on any other government contacts already initiated by the requestor;

(b) Explain that the query must be referred to NCIS Headquarters and that the NCIS Communications Directorate will contact the requestor to assist with the inquiry;

(c) Immediately notify your operational NCIS chain of command and Code 00C.

(4) Field personnel should refrain from offering comments on the merits of an inquiry, the character of a constituent, or speculating on the possible NCIS response.

d. Investigative Leads Involving Congress. In the event an investigative lead requires interaction with congressional members (senators, representatives, or staff), Code 00C should be notified immediately. Code 00C will coordinate and facilitate lead completion and may, on a case-by-case basis, accompany investigators on lead interviews involving congressional members or staff.

e. Incidental Contacts With Congress. If during the course of professional liaison activities or social activities an employee has incidental contact with congressional members and/or staff, during which questions regarding NCIS investigations, practices, or policies are raised, Code 00C should be apprised in a timely manner of the circumstances and the nature of the query. It is the policy of NCIS to endeavor to answer even informal expressions of interest in or concern about NCIS investigations and policies.

f. Personal Contact With Elected Representatives. In no way should Congressional Affairs guidance and policy provided above be construed as a restriction on the right of all NCIS personnel to communicate directly and in confidence with their elected representatives regarding unofficial and personal matters.

g. Legis Fellows Program. The NCIS Legis Fellows Program is a training program designed to offer senior experienced NCIS personnel the opportunity to train and work for up to one year on Capitol Hill, generally working as integral members on the staffs of senators, representatives, and congressional committees. The Program is administered for the DON by Navy OLA and the Navy Office of Civilian Human Resources (OCHR), and is managed for NCIS by Code 00C.

(1) NCIS is an active participant in the Navy's Legis Fellows Program. NCIS will solicit bids annually for the Legis Fellows Program. The Legis Fellows Program is highly competitive

and generally open only to GS-13 grade personnel. Application for the Legis Fellows Program is not a guarantee of nomination by NCIS for the Program, nor is it a guarantee that the candidate will be selected by the Navy for participation in the Program.

(2) Candidates for the Legis Fellows Program shall submit a nomination package in accordance with annual guidelines promulgated by Navy memorandum. Submitted packages will be reviewed by a board chaired by the Assistant Director of Communications or his/her designee. Upon senior management concurrence, approved packages will be forwarded to Navy OCHR for competitive selection.

(3) After selection for the Program, Legis Fellows are assigned to a training program for approximately three weeks. Code 00C provides administrative and funding/budgeting support to NCIS Legis Fellows during their training assignments. At the conclusion of training, Legis Fellows will seek and obtain one-year assignments to the staff of a congressional member or committee.

(4) While awaiting assignment to the congressional member or committee, NCIS Legis Fellows report operationally and administratively to Code 00C. Upon commencing their assignments with congressional staffs, NCIS Legis Fellows report operationally to the senator or representative to whom they are assigned, and administratively to Code 00C, which has responsibility for rating the Legis Fellows using input provided by the employing senator or representative. At the conclusion of the one-year assignment on Capitol Hill, Legis Fellows will generally return to a follow-on assignment in the Washington, D.C. area, frequently in Code 00C.

42-6. GOVERNMENT LIAISON

42-6.1. Code 00C has overall staff responsibility for all representational liaison involving DoD, other U.S. government agencies, foreign agencies, embassies and related public liaison, and agency representational duties. Such representational liaison activities are distinct from investigative or operational liaison activities undertaken by program managers or field personnel.

a. Code 00C duties include but are not limited to the following:

(1) Representational liaison activities involving the International Association of Chiefs of Police (IACP), the National Sheriff's Association (NSA), the International Police Organization (INTERPOL), the Liaison Officers Association (LOA), and other national and international law enforcement professional and technical associations organized to further law enforcement professional contact and success.

(2) Representational liaison with federal, state and local law enforcement agencies.

(3) Representational liaison with federal executive branch agencies, including intelligence agencies.

(4) Representational liaison with the foreign diplomatic community.

b. Code 00C is responsible for the design, purchase, and allotments of NCIS bulk memorabilia. Detailed instructions on NCIS bulk memorabilia are contained in NCIS-1, Chapter 37 Emergency and Extraordinary Expense Funds (EEE).

c. Code 00C has accountability for EEE funds relating to NCISHQ liaison.

42-6.2 Professional Association Memberships and Attendance at Conferences

a.. Memberships in professional associations are an excellent way to obtain training, to network, and to promote the NCIS mission. Attendance at professional conferences/seminars offers NCIS personnel unique training opportunities and stimulating environments in which to exchange information. It is important to point out, however, that professional association membership and conference attendance are two different issues, and legally must be handled differently.

b. Rulings by the U.S. Comptroller General and subsequent guidance from the U.S. Office of Personnel Management authorize law enforcement (LE) agencies to use appropriated funds to pay for agency memberships in professional associations that benefit the agency's LE mission, but only under certain conditions. The use of EEE Funds (formerly C&CI Funds) for the payment of membership dues in professional associations is prohibited.

c. Association memberships procured with appropriated funds must be obtained on behalf of the NCIS agency, and must be associated with a particular official position (e.g., DIR,NCIS) instead of an individual (e.g., Thomas Betro). The following conditions must be met:

(1) Memberships paid for with appropriated funds must be justified on the basis of a relationship to the authorized functions of the agency; and,

(2) Before funds are expended, a written justification must be prepared and retained for audit purposes; and,

(3) The membership remains with the position when the incumbent leaves the position; and,

(4) The membership is not for a position of management or control of the professional association; and,

(5) The incumbent in that position uses membership to improve the conduct, supervision, or management of his or her function within the agency.

d. It is recognized that many professional law enforcement associations exist at the national level, possibly warranting membership by NCIS. To be authorized, such memberships must strictly comply with established fiscal guidance, and payment for such memberships must be fully justified in writing, favorably endorsed by the SAC or appropriate Executive Assistant Director, and approved by Code 00C.

e. Among professional law enforcement associations, the International Association of Chiefs of Police (IACP) stands out because of its size and international reach. NCISHQ will authorize payment of

agency memberships in IACP on a limited basis. Payment for these memberships will be authorized only when the following conditions apply:

(1) The membership is for the positions of Director, Deputy Directors, Executive Assistant Directors, or Chief Psychologist; or,

(2) The incumbent in the position represents NCIS as a member of a committee, division or section of IACP, in which case approval will still be considered on a case-by-case basis; or,

(3) Other compelling reasons pertain, in which case NCIS personnel may present a written justification to the Assistant Director (AD), Code 00C for approval.

f. There is no prohibition on an employee's expenditure of personal funds to purchase an association membership.

g. The attendance of NCIS personnel at association conferences is a separate issue from that of membership. Attendance at a conference is recognized as a valid source of training and other opportunities. Currently, NCISHQ manages and funds the attendance of NCIS personnel at the following LE conferences in addition to the IACP: National Organization of Black Law Enforcement Executives; Women in Federal Law Enforcement; Hispanic American Police Command Officers Association; and the National Sheriff's Association. Unfortunately, it is not fiscally feasible to pay the expenses of all personnel who desire to attend the conferences held by these associations. With limited exceptions, Code 00C will solicit nominations via Gen Admin from each field office/code. The field office/code will e-mail the nomination, with a supervisor's endorsement, to the Code 00C events coordinator. Code 00C will select those personnel to attend, and will fund such attendance consistent with budgetary and other considerations. The NCIS Diversity Advisory Council will also be consulted on conference attendance.

h. In furtherance of the NCIS mission, field offices have the discretion of paying for association memberships and conference attendance in connection with state- and local-level professional associations within authorized budget constraints, and in compliance with the conditions specified above. The AD for Communication is the designated official for matters concerning payment for memberships in and attendance at conferences associated with national and international professional associations. The field office SAC is the designated official for matters concerning memberships in and attendance at conferences associated with state- and local-level associations. DADs will be the designated officials for matters concerning memberships in and conference attendance at state- and local-level associations for headquarters personnel. Conference participation may not be funded with EEE Funds.

42-6.3. Field Office Responsibilities. A primary responsibility of each SAC is to maintain professional relationships with all commands and other appropriate agencies within their assigned geographic area of responsibility. While the SAC is the primary contact for liaison, each field office will designate a primary and an alternate point of contact. Close working relationships with local military justice officials such as the Commanding Officer of the Trial Services Office (TSO), the Officer in Charge of the Marine Corps Legal Services Support Section (LSSS), the Marine Corps Regional and Base Staff Judge Advocates, and Senior Trial

Counsel are necessary. Regular and routine personal briefings of these individuals concerning ongoing investigations are very helpful to the overall liaison effort. The list below is by no means all-inclusive and is intended to highlight the crucial need for professional relationships with Navy and Marine Corps commands. Liaison with counterpart law enforcement and intelligence agencies is similarly important and the ideas below may be helpful in maintaining those important relationships:

a. Develop a listing of all commands, law enforcement agencies, and key personnel, updating as appropriate.

b. Correspond with ships/units returning from deployment, welcoming them home or to the area, and advise them of available NCIS services.

c. As feasible, develop a regular and recurring method of personally visiting the commanding officer, police chief, or other key members of serviced commands, and seek to identify and proactively respond to command priorities and pertinent operational or administrative issues.

d. Periodically attend staff meetings or other command functions in order to brief senior personnel on all elements of the NCIS mission and the full range of NCIS investigative, counterintelligence, combating terrorism programs, and other support services.

e. On occasion, personally deliver Reports of Investigation, various NCIS Public Affairs-related publications, or any other article that gives a reason to visit the command.

f. Invite Commanders/Commanding Officers to the NCIS field office to describe their command's mission, meet NCIS personnel, and discuss mutual expectations and requirements.

g. Encourage and reward creativity and initiative by NCIS employees who improve relationships with commands and other recipients of NCIS services.

h. Sponsor and/or participate in sporting and other liaison events.

i. Attend and speak at state and local law enforcement academies.

42-6.4. Fallen Officer Condolences. Each field office is responsible for sending Code 00C the names of law enforcement officers killed in the line of duty. In addition to the name, rank, and circumstances of death of the fallen officer, the name and address of the head of agency and spouse/family representative should be included. Code 00C will prepare condolence letters for the Director's signature for the fallen officer's department and spouse/family.

42-6.5 Death in the NCIS Family Notice. Each field office and headquarters code is responsible for providing Code 00C with timely information concerning the death of immediate family members of the NCIS employees within their respective office or code. Immediate family members include spouses, parents, siblings, and children. Information should include the full name of the deceased, their relation to the NCIS employee, time and date of viewing and/or funeral services, address to which condolence cards can be sent (usually the home of the NCIS

employee) and any details about charitable donations. Additional brief biographical information about the deceased may also be included. Code 00C is responsible for writing and disseminating the Gen Admin with this information. Field offices and headquarters codes should respect the decision of NCIS employees if they choose not to share this information.

42-6.6. Visitors to the Washington, D.C. Area. Field offices should submit names of visiting high-ranking police officials (foreign and domestic) to Code 00C so the department can assist with any liaison events, tours, or meetings with NCISHQ senior staff.

42-6.7. Liaison Program. Routine, official, and social interface with other agencies is necessary for a successful liaison program. NCIS personnel should be active in professional organizations, where it is possible to foster critical networking relationships and achieve increased visibility for NCIS. They should respond quickly and completely when counterparts in other law enforcement agencies request assistance. Moreover, NCIS personnel should invest time in getting to know professional counterparts, even if no current case or lead is being worked. Small amounts of time spent in liaison activities now can pay considerable dividends in the future.

APPENDIX (1): TYPES OF INFORMATION THAT CAN OR CANNOT BE RELEASED IN CONNECTION WITH AN INVESTIGATION OR AN EVENT

1. Information that can be released in connection with an investigation of a crime or event includes:

a. The type or nature of a crime or an event; and/or,

b. The location, date and time, injuries sustained, damages and a general description of how the incident occurred; and/or,

c. Type and quantity of property taken; and/or,

d. The identity of the victim (with the exception of sex crime victims) after next of kin have been notified; and/or,

e. Agencies conducting the investigation.

2. Information that cannot be released in connection with an investigation of a crime or an event includes:

a. Personal information, including names, about living persons that is obtained from a law enforcement record. Such information may be released only in compliance with the Privacy Act; and/or,

b. The identity of a suspect prior to arrest, unless such information would aid in apprehending the suspect or serve to warn the public of potential danger; and/or,

c. The identity of any victim of a sex crime or any related information that, if divulged, could lead to the victim's identity; and/or,

d. The identity of victims or witnesses if such disclosure would prejudice an investigation to any significant degree or place the victim in personal danger; and/or,

e. The identity of any juvenile who is a suspect or defendant in a case; and/or,

f. The identity of any critically injured or deceased person prior to notification of the next of kin; and/or,

g. The results of any investigative procedure such as lineups, polygraph tests, fingerprint comparison, ballistic test or other procedures; and/or,

h. Information which, if prematurely released, could interfere with the investigation or apprehension, such as the nature of leads, specifics of an "MO," details of the crime known only

to the perpetrator and NCIS, or information which may cause the suspect to flee or more effectively avoid apprehension; and/or,

i. Information that may be of evidentiary value in criminal proceedings; and/or,

j. Specific cause and manner of death unless officially determined by the medical examiner.

APPENDIX (2): TYPES OF INFORMATION THAT CAN BE RELEASED FOLLOWING AN ARREST OR THE FILING OF AN INDICTMENT

Information that can be released following the arrest, issuance of an arrest warrant, or filing of an indictment.

Per the JAG Manual, 0142 RELEASE OF INFORMATION PERTAINING TO ACCUSED PERSONS:

1. General. There are valid reasons for making information available to the public concerning the administration of military justice. The task of striking a fair balance among the protection of individuals accused of offenses, improper or unwarranted publicity pertaining to their cases, public understanding of the problems of controlling misconduct in the military service, and the workings of military justice, requires the exercise of sound judgment by those responsible for administering military justice and by representatives of the press and other news media. At the heart of all guidelines pertaining to the furnishing of information concerning an accused or the allegations against him is the mandate that no statements or other information shall be furnished to news media for the purpose of prejudicing the outcome of the trial of an accused person, or which could reasonably be expected to have such an effect.

2. Applicability of Regulations.

a. Except as provided in subsection 2. below, these regulations apply to all persons who may obtain information as the result of duties performed in connection with the processing of accused persons, the investigation of suspected offenses, the imposition of non-judicial punishment, or the trial of persons by court-martial. These regulations are applicable from the time of apprehension, the preferral of charges, or the commencement of an investigation directed to make recommendations concerning disciplinary action, until the imposition of non-judicial punishment, completion of trial (court-martial sessions), or disposition of the case without trial. These regulations also prescribe guidelines for the release or dissemination of information to public news agencies, to other public news media, or to other persons or agencies for unofficial purposes.

b. Judge advocates assigned by competent authority to represent an individual client other than the government shall comply with the applicable provisions of JAGINST 5803.1 series, (Rules of Professional Responsibility for Attorneys Practicing Under the Supervision of the Judge Advocate General) when making any statements concerning the subject matter of that representation. See, e.g., Rules 1.6 (Confidentiality of Information), 3.6 (Extra-Tribunal Statements), and 4.1 (Truthfulness in Statements to Others).

3. Release of Information.

a. As a general matter, release of information pertaining to accused persons should not be initiated by persons in the naval service. Information of this nature should be released only upon specific request and, subject to the following guidelines, should not exceed the scope of the inquiry concerned.

b. Except in unusual circumstances, information subject to release under this regulation should be released by the cognizant public affairs officer; requests for information received from representatives of news media should be referred to the public affairs officer for action. When an individual is suspected or accused of an offense, care should be taken to indicate that the individual is alleged to have committed or is suspected or accused of having committed an offense, as distinguished from stating or implying that the accused has committed the offense or offenses.

4. Information Subject To Release. On inquiry, the following information concerning a person accused or suspected of an offense, or offenses, may generally be released, without elaboration, except as provided in Subsection f.:

a. The name of the accused, the grade, age, unit, regularly assigned duties, duty station, and sex.

b. The general nature of the offense(s) of which the individual is accused or suspected. The fact that an accused has been charged with an offense may be released, but a statement explaining that the charge is merely an accusation and that the accused is presumed innocent until proven guilty must also be included.

c. The identity of the victim of any alleged or suspected offense, except the victim of a sexual offense.

d. The identity of the apprehending and investigating agency, and the identity of the counsel of the accused, if any.

e. The fact, time, and place of the apprehension of the accused.

f. The type and place of custody, if any.

g. Information that has become a part of the record of proceedings of the court-martial in open session.

h. The scheduling or result of any stage in the judicial process.

i. The denial by the accused of any offense or offenses of which he may be accused or suspected (when release of such information is approved by the counsel of the accused).

5. Prohibited Information. The following information concerning a person accused or suspected of an offense or offenses generally may not be released, except as provided in Subsection 6:

a. Subjective opinions, observations, or comments concerning the character of the accused, demeanor, credibility, or expected testimony at any time (except as authorized in subsection 4. e., or guilt of the offense or offenses involved.

b. The prior criminal record (including other apprehensions, charges, or trials) or the character or reputation of the accused.

c. The existence or contents of any confession, admission, statement, or alibi given by the accused, or the refusal or failure of the accused to make any statement.

d. The performance of any examination or test, such as polygraph examinations, chemical tests, ballistics tests, etc., or the refusal or failure of the accused to submit to an examination or test.

e. The identity or nature of physical evidence expected to be presented, or the identity, testimony, or credibility of possible witnesses, except as authorized in subsection 4.c. Particularly objectionable are statements or comments concerning information or evidence which is known, or which reasonably should be known, to be inadmissible before the tribunal.

f. The possibility of a plea of guilty to any offense charged or to a lesser offense and any negotiation or any offer to negotiate respecting a plea of guilty.

g. References to confidential sources or investigative techniques or procedures.

h. Statements or opinions regarding the credibility, reputation, motives, or character of DoD military or civilian officials.

i. Any other matter when there is a reasonable likelihood that the dissemination of such matter will affect the deliberations of an investigative body or the findings or sentence of a court-martial, or otherwise prejudice the due administration of military justice before, during, or after trial.

6. Exceptional Cases. The provisions of this section are not intended to restrict the release of information designed to enlist public assistance in apprehending an accused, or, suspect who is a fugitive from justice or to warn the public of any danger that a fugitive accused, or, suspected, may present. Further, since the purpose of this section is to prescribe generally applicable guidelines, there may be exceptional circumstances which warrant the release of information prohibited under subsection e, or the non-release of information permitted under Subsection d. Attention should be given to the SECNAV instructions implementing the Freedom of Information Act (5720.42E) and the Privacy Act (5211.5C). Consultation with the command judge advocate, if one is assigned, or with the cognizant trial services office concerning interpretation and application of these instructions is encouraged.

APPENDIX (3)

457288 15:21 20121203 IN:SSDEMAIL #103415 OUT:NCISWWSSD #748

GENERAL ADMINISTRATION 03DEC12

FROM: 0000 GEN: 11C-0025

TO: DIST

SUBJ: NCIS POLICY DOCUMENT 12-14: ADMINISTRATIVE (NCIS RETIREMENT GEN ADMINS)

REFERENCE
(A) NCIS-1, Chapter 42, Public Affairs: Media Relations, Congressional Affairs, and Law Enforcement Liaison of Sep 08

1. Effective immediately, the Communications Directorate (Code 00C) is responsible for drafting and releasing all retirement announcements. Code 00C will prepare standardized retirement Gen Admins sent throughout the NCIS organization.

2. NCIS headquarters codes and field offices shall send retirement information to Code 00C two weeks prior to the retirement date.

3. Send retirement information using the "NCIS_Retirement_GEN" group e-mail address (b)(7)(E) @navy.mil) located in the NMCI global address list. Provide the following information:

a. Name

b. Identify the current career field (special agent, professional staff, support personnel - be specific)

c. Date of retirement

d. Number of years with NCIS

e. Previous military, law enforcement, or Federal Government service (optional)

f. Position title and location of the initial NCIS assignment

g. Other NCIS assignments to highlight

h. Final NCIS assignment

i. Proudest accomplishment

j. Future plans (employment in new career field, travel, full-time retirement, etc.)

k. Name of spouse and children (optional)

l. Forwarding address or contact information (optional)

m. Plan for retirement ceremony or celebration (optional)

4. This policy will be incorporated into the next revision of reference (a).

5. The point of contact for this policy is Communications Director (b)(7)(E) navy.mil or (b)(7)(E) or Public Affairs Specialist (b)(7)(E) @navy.mil or (b)(7)(E)

DISTRIBUTION
NCISHQ: All Directorates and Departments
INFO: WWSSD

CHAPTER 43
TITLE: FOREIGN AREA OFFICER (FAO) PROGRAM
POC: CODE 24
DATE: SEP 09

REFERENCES:
(a) DoDI 5160.70, "Management of DoD Language and Regional Proficiency Capabilities," June 12, 2007
(b) DoD Joint Travel Regulation, Volume 2
(c) NCIS-1, Chapter 38, "Permanent Change of Station (PCS)," December 2006

APPENDICES:
(1) Defense Language Aptitude Battery Qualifying Scores
(2) Example Foreign Area Officer Individual Development Plan

43-1. INTRODUCTION

43-1.1. The Naval Criminal Investigative Service (NCIS) created the FAO Program in April 2007. The purpose of the NCIS FAO program is to educate, train and maintain, through career management and continuing education, a group of qualified special agents and intelligence specialists who possess, or will possess, specific skills and knowledge. The Navy and Marine Corps are globally distributed and forwardly deployed; therefore, FAOs will carry out the traditional missions of NCIS, predominately in foreign locations. NCIS' ability to provide effective, world-wide counterterrorism (CT), counterintelligence (CI) and criminal (Crim) investigative support to the Department of the Navy (DON) depends largely on its ability to operate effectively across a broad spectrum of foreign environments and in a variety of cultural backgrounds. NCIS must develop and maintain productive relationships with the law enforcement agencies and security services of international partners; this is accomplished by personnel with extensive cross-cultural competencies and language skills. Participation in the FAO program is voluntary, and it is open to qualified non-management and management personnel.

43-1.2. FAOs receive advanced academic studies and language training related to specific geographic regions through an adaptive and flexible training curriculum that incorporates studies from recognized U.S. Government, Department of Defense (DoD), and civilian training and educational institutions. FAOs will become knowledgeable professionals with a focus on law enforcement and security. Persons selected into the FAO program will focus their training, education and assignments on a single region. A combination of academics, operational training,

in-country and regional assignments will prepare, develop and maintain advanced knowledge in specific geographic areas or countries.

a. A Middle East FAO will receive language training in Arabic, graduate-level education in Middle Eastern affairs and culture, and assignments in the Middle East region. Assignments outside of the Middle East will likely be for training, education or for duty in continental United States (CONUS) positions where his or her Middle Eastern expertise can be utilized. In most cases, the Middle East FAO will return to the Middle East for follow-on assignments, most likely of increasing complexity.

b. Career tracks for other area specialties will be similar. Transfer to positions where a given FAO's expertise has little utility is unlikely. Opportunities for extended overseas assignments are possible, but approval will be contingent on the goals and objectives of operational programs, personal career development and individual performance.

43-1.3. FAOs are recruited from National Security Personnel System (NSPS) special agents 1811s and Defense Civilian Intelligence Personnel System (DCIPS) Intelligence Specialists 0132s, including those commonly referred to as Intelligence Analysts and Intelligence Operations Specialists. New employees with existing language skills or area expertise may be recruited for the FAO program. These employees are required to complete a defined period of employment with NCIS, currently two years, before they are eligible to enter the program. In exceptional cases a waiver to this requirement is possible. In all instances, an FAO will be a NCIS Special Agent or Intelligence Specialist with assigned duties consistent with those positions. A FAO can be assigned primary responsibilities associated with any of the operational disciplines (CI/CT/Crim), Cyber or the Directorate of Intelligence. FAO skills should be viewed as an additional set of enablers that enhance the capabilities of an individual to conduct CT, CI or Crim activities in a cross-cultural environment. These skills will be used to facilitate operations in foreign locations, to inform commands and NCIS in matters related to his or her regional specialty, and to facilitate partnerships with foreign law enforcement and security services.

43-1.4. To support DON objectives, the NCIS FAO regional specialty tracks reflect those geographic regions of strategic interest to the Navy and Marine Corps. The selection and placement of FAOs are linked to NCIS' strategic goals and operational needs, as well as the strategic objectives of DON. Regional specialties for the NCIS FAO program presently include Africa (sub-specialties include West, Central, North and Sub-Sahara Africa), Europe (sub-specialty Eurasia), the Middle East, Southeast Asia, the Far East and Latin America.

43-2. ELIGIBILITY

43-2.1. NCIS special agents and intelligence specialists are eligible for participation in the FAO program provided they meet the following criteria:

a. NCIS special agents and intelligence specialists must have a minimum of 2 years of service with NCIS. The 2 year service date is determined by the employee's hire date. The minimum 2 year service requirement may be waived by the FAO program manager if the applicant is assessed to possess exceptional qualifications relevant to the FAO field.

b. A Bachelor's degree from an accredited college or university.

c. Possess foreign language skills in a language that is dominant or commonly used within his or her region of interest as determined by the FAO program office. Proficiency in the language must be documented by a Defense Language Proficiency Test (DLPT) minimum score or Oral Proficiency Interview score of 2 in at least two of the measured skills (2/2 in speaking, reading and/or listening) on the Interagency Language Roundtable (ILR) scale. DLPT scores must be current within 1 year. The DLPT must also be the most current version available for the language in question. FAO candidates who lack documented proficiency in a foreign language used within their area of interest may be eligible for the FAO program and for language training if they possess a qualifying Defense Language Aptitude Battery (DLAB) score. Qualifying DLAB scores vary depending on the language. Qualifying scores for the language and the categories for which they are associated with are provided at Appendix (1). Continued inclusion in the FAO program by all participants requires a yearly DLPT with minimum scores of 2/2 or better.

d. Sign the NCIS mobility agreement and be subject to transfer according to the needs of the service. FAO candidates and program participants must be willing and capable of serving in an overseas assignment in the geographic area of their specialty and must continue to maintain the conditions necessary to serve in overseas assignments throughout their participation in the program. NCIS FAOs and applicants must also be willing to accept assignment to any location within the geographic area of their specialty. FAOs or FAO candidates should have no impediments to moderate or long term (approximately 12-18 months) temporary assignments or relocation for training and education purposes.

e. FAO candidates and program participants must also maintain their eligibility for a Top Secret/Special Compartmented Information security clearance and access to classified information.

43-3. SELECTION PROCEDURES

43-3.1. Selection into the FAO program is a competitive process. Periodically, announcements will be published by the FAO program office requesting application by interested parties. In response, applicants will forward an application package consisting of the information listed below. Applicants must declare a regional specialty area for which they are seeking selection. Selection will be based on an applicant’s overall professional performance and qualifications as documented by (1) performance evaluations, (2) Special Agent in Charge (SAC) or Deputy Assistant Director (DAD) recommendations, (3) foreign language proficiency or aptitude, (4) relevant political, military or area studies education, and (5) practical exposure to the geographic area of interest. The FAO program office reserves the option to interview FAO candidates and their supervisors concerning the candidate’s qualifications. The FAO application package consists of the following materials:

a. Letter to the FAO program manager stating applicant’s interest in specific regional area(s), highlighting candidate’s professional accomplishments, foreign area, language education, and experience.

b. College or university transcripts (to verify applicant's eligibility for admission into a graduate degree program) and other documentation that supports the candidate's applicable education, training and experience.

c. SAC or DAD endorsement and recommendation regarding the candidate's inclusion in the FAO program.

d. DLPT scores dated within one year of the application. DLAB scores are also acceptable and are not required to be less than one year old.

43-3.2. Applications will be reviewed by the FAO program office to ensure completion of basic qualifications. Information concerning qualified candidates will be presented to the FAO selection board for nomination into the program. Prior to the selection board, the FAO program manger will query operational directorate heads, impacted geographic Executive Assistant Directors (EAD) and the Directorate of Intelligence, as well as others, to determine priorities pertaining to regional focus areas. The query will be conducted to assist in identifying requirements for FAOs by area specialties and quantity. The FAO selection board will be chaired by the FAO program manager. Other members will include a DAD from the Criminal, Counterintelligence and Combating Terrorism Directorates, a senior representative of the Directorate of Intelligence, the Personnel Services and Operations Department and the NCIS Diversity Officer. Nominations by the selection board will be forwarded, via the Deputy Director for Operations and the Deputy Director for Management and Administration, to the Director, NCIS for awareness and concurrence with the board decision. The FAO program office will announce the FAO selection results by General Administration document.

43-4. INDIVIDUAL DEVELOPMENT PLAN (IDP)

43-4.1. A flexible training curriculum is mandatory, due to the broad scope of languages and cultural awareness required by FAOs, along with their varied level of existing skills, experiences and assignments. As a result, IDPs are created for each FAO and are updated annually. IDPs serve as a guideline for FAO training, education and career development. An example IDP is provided at Appendix (2).

43-4.2. IDPs are drafted by a FAO action officer and coordinated with the FAO program manager, the field managers, headquarter programs, and the FAO. The coordination of the IDP is a critical component of the FAO program. Once coordinated, all efforts to proceed in accordance with an IDP will be made.

43-5. CAREER PROGRESSION, ASSIGNMENTS, TRAINING AND FAO COMPETENCY

43-5.1. FAO career progression and assignment protocol is a process that allows an FAO to become a subject matter expert in their selected foreign area or country. Career progression in non-supervisory and non-management positions includes positions in the NSPS Investigative (YK) pay band 1 with promotion opportunity to pay band 2. Management positions include those in Supervisor/Manager (YN) pay band 2 and 3. For DCIPS employees, career progression

and management track follow the identical pay band and both non-supervisors and supervisors have promotion opportunities from DCIPS pay band 2 through 5.

43-5.2. Newly selected FAOs without relevant area-studies, education, cultural experience and minimal or no foreign language proficiency will be required to complete language school, area studies courses and seminars. FAOs will be assigned to positions that provide the best opportunity to develop experience in their area of focus. Examples of such assignments can include, but are not limited to, serving in a foreign NCIS field office, a force protection detachment, a joint terrorism task force, a staff position at a combatant or key naval command, a position within the Counterintelligence and Combating Terrorism Directorates, a CONUS-based field office having OCONUS responsibilities, or where mission requirements call for FAO-related skills and experience. All FAO assignments will be coordinated with the geographic EADs to ensure maximum impact on global and regional priorities.

43-5.3. During their tenure in the FAO program, FAOs will be assigned to receive post-graduation education if they do not already possess an equivalent degree in a subject related to their area focus. Typically, this education is received at the Naval Post Graduate School or at another recognized graduate program. Upon completion of advance studies, FAOs will return to the field and continue to serve in FAO-oriented assignments.

43-5.4. Training and education sources currently utilized by the FAO program include the Naval Post Graduate School, Monterey, CA and the DoD Regional Security Centers. These centers include the George C. Marshall Center for Security Studies in Garmisch, Germany, the Asia Pacific Center for Security Studies in Honolulu, HI, the Center for Hemispheric Defense Studies, the Near East-South Asia Center for Security Studies, and the Africa Center for Security Studies in Washington, D.C. Also utilized are the Foreign Service Institute in Arlington, VA, and the Defense Language Institutes in Washington, D.C. and Monterey, CA.

43-5.5. Selection as an FAO does not exclude an individual from pursuing supervisory and management positions. Accession of FAO-qualified special agents and intelligence specialists to management positions is encouraged, as those with in-depth knowledge of foreign areas are required in many NCIS management and leadership positions. In the interest of fostering overall career development, FAOs in management career tracks may require assignment to positions outside their FAO specialty. However, efforts will be made by the FAO program manager to have both non-managers and managers spend the predominate portion of their career in their area of interest. It is envisioned that FAOs will typically rotate between CONUS assignments and their designated foreign area or country, with assignments that provide professional growth and development throughout their career.

43-5.6. The objective of the FAO program is to achieve, at a minimum, language, regional expertise and cultural competency (LREC) skills consistent with the professional level (Level 3) as defined by reference (a) for all program participants. This proficiency level typically requires 2 to 4 years of work experience focused on a particular region or country of interest. Individuals at this level are considered valuable resources for information concerning trends and issues related to their geographic specialty. They are capable of writing and presenting overviews and focused briefings concerning their area of specialization. Their cultural experience reflects the

knowledge of someone who has lived in the region or country for a year or more and has been immersed in the culture. Typically, the professional level individual has a foreign language capability at the level 2+ to level 3 on the ILR scale in at least one language dominant in the country or region. The overarching goal of the FAO program is to produce NCIS FAOs with language skills at the 3/3 level. The professional level employee's knowledge comes from a combination of education, prior military or work experiences, area-studies courses, in-country assignments, travel, mentoring and specialized professional experience.

43-5.7. Development of LREC skills consistent with the senior professional level (Level 4), defined by reference (a), is anticipated and expected of senior FAOs. Individuals at this level typically possess 4 to 7 years of experience in a specialized area and have general experience in a broader subject area. For NCIS, this experience may be the conduct of criminal investigative, counterintelligence or counterterrorism activities or analysis within the context of their regional area of focus. Senior level professionals have a deep knowledge and understanding of their region or country of interest, contribute viewpoints on complex matters, aid in the development of policy and have experience working directly with senior U.S. military and policy officials on programs that affect U.S. policy in that region or country. The cultural knowledge of a senior professional allows him or her to easily blend in with the culture and has a language capability at the level 3/3 or higher. Knowledge comes from a combination of advanced graduate education, seminars, research, area-studies courses, in-country assignments, travel, mentoring, and specialized professional experience. The senior professional may be called upon to teach on the subject and could be published.

43-5.8. Due to the extensive investment in training and education, as well as the extensive period of time required to gain sufficient expertise, acceptance of a position in the FAO program implies a minimum 5 year commitment to the program. Further, acceptance of long-term training and educational benefits may require the completion of a continuing service agreement. As a rule, a continuing service agreement mandates at least 2 years of federal service when completion of the training or education received is in excess of 1 year.

43-5.9. On a case-by-case basis, non-FAOs may receive FAO program sponsored training or education. This training and education is provided in cases where language or regional proficiency will enhance specific mission functions to be conducted by the employee. Receipt of training and education under these conditions does not constitute acceptance into the FAO program.

43-6. MOBILITY AND TEMPORARY DUTY

All FAO movements will be conducted in accordance with the DoD Joint Travel Regulation, reference (b). Additional information concerning permanent change of station and temporary change of station moves can be found in NCIS 1, Chapter 38, "Permanent Change of Station (PCS)", reference (c).

Pages 1047 through 1048 redacted for the following reasons:
- -
(b)(5)

NCIS-1, CHAPTER 44
NCIS MANPOWER MANAGEMENT PROGRAM
EFFECTIVE DATE: SEPTEMBER 2014

Table of Contents: **PAGE**

Current Policy Gen Admin:
(a) GEN 14P-006 (Interim Position Management Board Submission Process), dated 20 Sep 11

References:
(a) OPNAV Instruction 1000.16K CH-1, Navy Total Force Manpower Policies and Procedures, 4 October 2011

44-1. Purpose

a. This chapter provides guidance, assigns responsibility, and establishes policy and procedures for manpower management. Decreasing resources, continuing operational demands, and the dynamic personnel environment within the Naval Criminal Investigative Service (NCIS) necessitates a disciplined and collaborative approach to manpower management. This chapter outlines the annual process for managing the creation, allocation, and restructuring of billets and organizational elements within the agency.

b. This chapter applies to all civilian and military billets within NCIS.

c. For each NCIS Headquarters (NCISHQ) directorate and field office, the validated billet structure serves as the baseline for billet management and the function performed by each billet.

d. The process for implementing changes to the billet structure is designed to support the special agent transfer cycles, resource constraints, and out-of-cycle billet change requirements.

e. Manpower management processes provide special agents in charge (SACs) and deputy assistant directors (DADs) with a tool to manage their human capital while maintaining the business process discipline needed to manage resources.

44-2. Policy

a. Manpower management is a dynamic process intended to obtain maximum process efficiency and organizational effectiveness within each functional element of the organization. Sound manpower management requires a continuous balance of mission requirements,

operational priorities, program needs, and workload (level of effort), as well as coordination, communication, and collaboration.

b. The NCIS manpower management process is designed to advise program managers and field office personnel on the current status of resources that affect billet establishment, disestablishment, allocation, and alignment. All proposed reorganizations, requests for billet changes, or realignments must reflect sound business practices and support mission priorities. Actions must be consistent with reference (a) and the Navy's authoritative manpower system, Total Force Manpower Management System (TFMMS), and should reflect a force structure that supports required level of effort across NCIS.

44-3. Cancellation

a. Policy Gen Admin 14P-006, Interim Position Management Board Submission Process, 20 September 2011.

b. NCIS Manual 1, Chapter 44, Position Management Program, 8 December 2008.

44-4. Chapter Sponsor. NCIS Manpower Department (Code 14P).

44-5. Definitions

a. Program manager (PM). Headquarters managers who have program or project responsibility to man, train, and equip (MTE) NCIS manpower resources. PMs are located at NCISHQ in Code 00, Code 10, Code 11, Code 14, Code 15, Code 22, Code 23, and Code 25.

b. Level of effort (LOE). Measurable effort expended in performance of assigned mission-related functions and tasks.

c. Manpower personnel. People assigned to Code 14P with authority to change the NCIS force structure and submit information to TFMMS.

d. Billet. A required and authorized (funded) manpower position with assigned criteria that define the duties, tasks, and functions to be performed, and the specific skills and required skill level to perform those functions. A billet is represented by a unique number called a billet identification number, or BIN.

e. Manpower management. Planning, balancing, modifying, and approving a manpower billet structure to ensure operational readiness in accordance with an organization's priorities.

44-6. Program Objectives

a. The goal of manpower management is to manage the resources for organizational billet or position assets in a manner promoting agency efficiency and effectiveness. Program integrity will be maintained throughout all organizational elements.

b. Manpower Management Process Business Rules

(1) The approved billet structure is maintained on Lighthouse at the Code 14P Manpower shared site. The current approved billet structure with names is posted monthly on Lighthouse. This is the authoritative structure to be used by all NCIS activities for requesting hiring actions and for planning transfers and promotions.

(2) Billet changes normally will be addressed during two periods each year: in the summer (Primary Force Structure Review—main adjustments to begin preparing for the next promotion/transfer cycle) and in the winter (Secondary Force Structure Review—adjustments just prior to overseas extension decisions and the beginning of the promotion/ transfer cycle).

(3) Resource sponsor funding reductions or additions may require out-of-cycle adjustments to the billet structure.

(4) NIP and MIP billets are programmed by project, making them ineligible for funding exchanges.

(5) Only PMs are authorized to submit changes to billets. PMs are responsible for coordinating all actions (i.e., changes, reductions, or additions) with requisite field office personnel and other PMs, as appropriate.

(6) Billet changes should be based on PM review of Field Office Reporting (LOE/production), billet criteria (description, location), and/or funding. The function and location of a billet determine that billet's relevance to the NCIS force structure; personnel assignments should be based on the required structure.

44-7. Responsibilities and Process

a. Transfer Cycle Planning/Primary Force Structure Review

(1) The majority of billet changes to align LOE for the next transfer cycle should be accomplished after the Field Office Reporting reviews before the start of the spring/summer transfer cycle.

(2) PMs must follow the Manpower Management Business Rules in paragraph 44-6b.

(3) PMs must conduct all coordination regarding a billet change with appropriate offices (e.g., field offices, geographical executive assistant directors (EADs), and other Headquarters activities) and ensure assistant directors (ADs) and EADs concur before submitting specific changes to Code 14P, Manpower. Field office support officers (FOSOs) must coordinate all billet change requirements with the appropriate MTE PM(s) after internal coordination and approval at the SAC/EAD level.

(4) Changes will be submitted by annotating the current official billet structure (on Lighthouse). The change must show which billet criteria is to be changed (i.e., the "Change To" line) immediately below the current billet criteria (i.e., the "Change From" line). After emailing the submission of the annotated structure, PMs must schedule a meeting with Manpower

personnel to ensure all changes will be completed in the most effective and efficient manner. This process is outlined in Appendix A.

(5) Manpower personnel will prepare a confirmation document based on the submitted information and forward the document to the PM within three days of the meeting.

(6) PMs must review the confirmation document and respond in writing (via email and copying ADs and EADs) for documentation purposes. PMs and Manpower will reconcile any discrepancies in a reasonable amount of time (e.g., within 30 days of the original submission).

(7) Manpower personnel must provide a summary of requested changes to the Principal Executive Assistant Director (PEAD). The PEAD will brief the proposed billet changes to the Deputy Director for concurrence/approval.

(8) Upon the Deputy Director's approval, Manpower personnel will make appropriate changes in the manpower document, submit changes to TFMMS, and ensure legacy documents are properly archived.

(9) Manpower personnel will notify PMs and FOSOs when a new billet structure is posted on Lighthouse.

b. Transfer Cycle Adjustments/Secondary Force Structure Review/Billet Adjustments

(1) Based on end-of-year reporting (and resulting operational trends), PMs will have the opportunity to realign or modify billets to meet operational priorities and to ensure the appropriate positions are announced during the transfer cycle notification process.

(2) PMs must follow the Manpower Management Business Rules in paragraph 44-6b (e.g., using the current billet document on Lighthouse) and the published review of the most recent program and field office evaluation reports from Code 14A, Planning and Evaluation.

(3) PMs must use the procedures identified for the Primary Force Structure Review in paragraph 44-7a.

c. Resource Sponsor Adjustments/Billet Summit (As Required)

(1) Increases and decreases in resources routinely occur. For all instances in which the changes are known, Manpower personnel will provide PMs with specific changes in projects so that they may be addressed during the Secondary Force Structure Review in the summer. In general, increases to billets are directed toward specific programs or projects. Reductions, particularly against Security and Investigative Activities funding, require an NCIS executive leadership consensus on which billets to reduce. A "billet summit" will be used to reach consensus. Billet summits will be convened by the Deputy Director or PEAD, as required.

(2) Manpower personnel will begin the resource adjustment process by notifying the PMs of the required reductions. PMs must follow the Manpower Management Business Rules in paragraph 44-6b for increases, decreases, and any re-alignments due to funding changes.

(3) After input is received from the PMs, the Code 14P DAD will conduct a planning meeting with the PEAD and then coordinate a billet summit with NCIS senior executives. Codes 00 through 25 and Global Ops will be included in the summit to ensure full MTE representation. Codes 02A and 02P will be included in the summit for visibility in their areas of responsibility.

(4) Resource sponsor adjustment decisions will be made in the billet summit. Because billet summit attendees will determine reductions to the NCIS force structure, the Deputy Director (or designee with delegated authority) must be present.

(5) Manpower personnel will ensure all adjustments are captured and document any realignments required from directed changes. Manpower personnel will prepare a confirmation document of the decisions made in the billet summit and send it to the PMs, ADs, EADs, and Chief of Staff within two days of the summit.

(6) PMs must review the billet summit documentation and respond in writing (via email and copying relevant ADs and EADs) for documentation purposes. PMs and Manpower personnel must reconcile any discrepancies.

(7) Manpower personnel will provide the PEAD with the final documentation of the reductions and adjustments. Any requested deviations from decisions made in the billet summit will be highlighted for Deputy Director approval.

(8) Manpower personnel will make appropriate changes in the manpower document, submit changes to TFMMS, and ensure legacy documents are properly archived in Lighthouse.

44-8. Manpower Reporting Requirements

a. In order to record program and billet decisions for historical purposes and to compare historical data, it is necessary to employ standardized information recording.

b. Manpower personnel shall post the following documents on Lighthouse each month:

(1) Current month billet structure with names (sort- and filter- capable).

(2) Funding summary (by Project).

(3) Billet summary (by Location and Project).

(4) Listing of any newly created billets (as applicable).

(5) Listing of any deleted billets (as applicable).

(6) Listing of any billet changes (as applicable).

c. Manpower personnel must maintain archives of manpower data reports so that all billet information is available for viewing and researching, in accordance with DoD and Navy records management requirements.

APPENDIX A
RECORDING BILLET CHANGES

1. In the current official billet structure (posted on the Code 14P site on Lighthouse), locate the billet you want to change and copy it.

2. Paste the entire billet record to a new excel spreadsheet, recording your billet changes to submit to 14P Manpower.

3. Copy and paste the selected row directly below. This results in two rows for the same billet on your submission document.

4. Make the desired changes to the second row of the billet for each billet you want to change and make the **font red**. The billet is displayed as it currently exists and with the requested changes.

5. Leave one blank row between each billet change set.

Example: It is determined that the manpower function will be assigned to the Far East Field Office for execution. This results in the billet for manpower being realigned to the Far East Field Office. This example assumes the incumbent will be placed in another billet at NCISHQ.

Step 1: Locate the billet.

UIC	ACTY	BIN	MTE	BILLET TITLE	FUND/ PROJECT	SER	GR	NAME
63285	NCISHQ	3620750	14P2	MANPOWER OFFICER	F1A MHA	00343	14	

Step 2: Copy and paste the billet record onto a new spreadsheet.

UIC	ACTY	BIN	MTE	BILLET TITLE	FUND/ PROJECT	SER	GR
63285	NCISHQ	3620750	14P2	MANPOWER OFFICER	F1A MHA	00343	14

Step 3: Copy and paste the billet record to create two rows of the same billet.

UIC	ACTY	BIN	MTE	BILLET TITLE	FUND/ PROJECT	SER	GR
63285	NCISHQ	3620750	14P2	MANPOWER OFFICER	F1A MHA	00343	14
63285	NCISHQ	3620750	14P2	MANPOWER OFFICER	F1A MHA	00343	14

(b)(7)(E)

Step 4: Make changes in red to second row.

UIC	ACTY	BIN	MTE	BILLET TITLE	FUND/ PROJECT	SER	GR
63285	NCISHQ	3620750	14P2	MANPOWER OFFICER	F1A MHA	00343	14
0765A	**FEYK**	3620750	14P2	MANPOWER OFFICER	F1A MHA	00343	14

VACANT

CHAPTER 45
TITLE: MANAGING INVESTIGATIONS AND OPERATIONS
POC: CODE 00I
DATE: OCT10 (11/12)

POLICY DOCUMENT:

APPENDIX (13): Gen Admin 11C-0024 of 15 Nov 2012 released NCIS Policy Document 12-13: Administrative (Implement Standardized Case Review Sheet). Policy Document 12-13 contains revised or new policy that has not been incorporated into this chapter and should be reviewed in its entirety.

45-1. GENERAL

Conducting investigations and operations in a timely and thorough manner is critical to successful accomplishment of the Naval Criminal Investigative Service (NCIS) mission. This chapter describes and assigns responsibility for management processes that are necessary to maintain the quality of NCIS' investigative and operational activities.

45-2. QUALITY STANDARDS FOR INVESTIGATIONS

45-2.1. General Standards. NCIS investigations will be conducted in accordance with the President's Council on Integrity and Efficiency/Executive Council on Integrity and Efficiency (PCIE/ECIE) Quality Standards for Investigations (http://www.ignet.gov/pande/standards/invstds.pdf)
The three general standards are:

a. Qualifications. Individuals assigned to conduct investigative activities must collectively possess the professional proficiency for required tasks.

b. Independence. In all matters relating to investigative work, the investigative organization must be free, both in fact and appearance, from impairments to independence; organizationally independent; and must maintain an independent attitude.

c. Due Professional Care. Due professional care must be used in conducting investigations and preparing related reports. This standard requires a constant effort to achieve quality professional performance and includes:

(1) Thoroughness. All investigations must be conducted in a diligent and complete manner. Reasonable steps will be taken to ensure pertinent issues are sufficiently resolved, and that all appropriate criminal, civil, contractual, or administrative remedies are considered.

(2) Legal Requirements. Investigations will be initiated, conducted, and reported in accordance with all applicable laws, rules, and regulations, including NCIS policy and procedures.

(3) Appropriate Techniques. Specific methods and techniques used in each investigation must be appropriate for the circumstances and objectives.

(4) Impartiality. All investigations must be conducted in a fair and equitable manner, with the perseverance necessary to determine the facts.

(5) Objectivity. Evidence must be gathered and reported in an unbiased and independent manner in an effort to determine the validity of an allegation or resolve an issue.

(6) Ethics. At all times, actions of the investigator and NCIS must conform to generally accepted standards of conduct for government employees.

(7) Timeliness. All investigations must be conducted and reported with due diligence and in a timely manner. This is especially critical given the impact investigations have on the lives of individuals and activities of organizations.

(8) Accurate and Complete Documentation. Investigative reporting and investigative accomplishments (indictments, convictions, recoveries, etc.) must be supported by adequate

documentation (investigator notes, court orders of judgment and commitment, suspension or debarment notices, settlement agreements, etc.) in the case file.

45-2.2. Qualitative Standards. In addition to the three general standards, there are four qualitative standards that must be addressed if an investigative effort is to be successful. These standards are:

a. Planning. Establishing case specific priorities and developing objectives to ensure that individual tasks are performed efficiently and effectively.

b. Execution. Conducting investigations in a timely, efficient, thorough, and legal manner.

c. Reporting. Reports (oral and written) must thoroughly address all relevant results of the investigation and be accurate, clear, complete, concise, logically organized, timely, and objective.

d. Information Management. Investigative data must be stored to ensure effective retrieval, reference, and analysis.

45-2.3. Investigative Leadership and Support. NCIS personnel conducting investigative activities must have the authority to conduct the activity and the requisite professional proficiency.

a. Special agents carry out the full range of duties associated with criminal investigations, counterintelligence activities, and other related activities. Non-special agents (i.e., investigators, investigative review specialists, intelligence specialists, and professional administrative staff) also perform investigative, analytical, and security functions in support of the NCIS mission.

b. Case control agents for criminal investigations must be credentialed civilian or military special agents. Special agents who have not been certified by their special agent-in-charge (SAC) as having successfully completed field training indoctrination may serve as case control agents under the supervision of a field training agent (FTA) or supervisory special agent (SSA). Non-special agents may act as case control agents for reporting details and disposition of incidents that do not require a full NCIS criminal investigation, as well as reciprocal and specific-phase investigations.

c. Non-special agents may conduct investigative tasks to support the case control agent. In assigning investigative tasks to non-special agents, case control agents and their supervisors should take steps to limit the non-special agents' exposure to personal danger/physical confrontation while conducting the investigative tasks. Special agents should conduct the investigative tasks that may require the use of deadly force and/or result in physical confrontation. SACs, assistant-special-agents-in-charge (ASACs), and SSAs should consider the safety of non-special agent personnel prior to using such personnel to conduct certain dangerous investigative tasks. The lack of availability of a special agent is not sufficient rationale to allow a non-special agent to conduct an investigative task where the likelihood of needing deadly force or having a physical confrontation is probable.

d. Non-special agents are authorized to assist special agents in executing search warrants when specifically authorized by the SAC or deputy assistant director (DAD).

e. Those persons accredited by the Director, NCIS as special agents, investigators, and operational representatives are authorized to administer oaths and take sworn statements. This authority applies only to official investigative duties in connection with the investigative jurisdiction of NCIS, as set forth via Uniform Code of Military Justice (UCMJ) Article 136 (10 United States Code (USC) 936) and 5 USC 303.

45-2.4. Timeliness

a. Reporting timeliness is a critical requirement for our customers, thus the following metrics are established for criminal investigations and leads. Time to complete a case is measured from case initiation to presentation for adjudication, or case closure, if no adjudicative action is taken.

Investigative Category	Timeliness Metric
Category 3, 4, 5, 6, 7, and 8 investigations	90% complete within 90 calendar days.
Leads/Actions	90% complete within 10 business days. 99% complete within 30 calendar days.

b. It is understood that certain complex investigations, such as procurement fraud, espionage, etc., may require a much longer time period to bring to a successful conclusion. These metrics are standards that we should strive to achieve, but we must not compromise thoroughness or quality to meet these standards.

45-3. FIELD OFFICE RESPONSIBILITIES

45-3.1. Investigative Plan. Upon receipt, each complaint must be evaluated against the NCIS mission, priorities, and guidelines for one of three decisions:

a. Initiate investigative activity;

b. Take no further investigative action; or

c. Refer to another appropriate authority (note: when NCIS receives a criminal complaint and refers that complaint to another agency (i.e., local/base police), a Report of Investigation (ROI (INFO)) detailing the information and reason for referral must be submitted to NCIS Headquarters (HQ) within 10 days).

45-3.2. If the SSA, ASAC, or SAC decides to initiate an investigation, case agents will begin necessary and immediate actions to include establishing an investigative plan of action that includes as many of the following steps as deemed necessary:

a. Determine the primary nature of the allegations (criminal, civil, and/or administrative).

b. Identify possible violation(s) of law, rule, or regulation, and understand corresponding elements of proof or standards.

c. Establish the objectives of the investigation. Care must be taken in stating the objectives of the investigation; i.e., the initial objective of most investigations, if not all, is to determine if a crime has been committed.

d. Coordinate the decision to open an investigation with appropriate authorities if warranted (i.e., Federal Bureau of Investigation, local police).

e. Determine applicable judicial/administrative venue and coordinate with prosecutors/ adjudicators when appropriate.

f. Identify and prioritize steps necessary to meet investigative objectives, which include identifying the best investigative approach to resolve allegation(s) or issue(s) (i.e., list of witnesses, relevant records).

g. Determine resources necessary to meet investigative requirements.

h. Establish a time-phased approach that ensures leads are pursued in a timely manner. As soon as the case is initiated, the SSA will discuss planned investigative action with the case agent. Within three working days of opening the investigation, the agent, in conjunction with the SSA, will formalize a written investigative plan. It is understood that the investigative plan is a "living" document to be modified and updated as appropriate during the pendency of the investigation. As such, the SSA will continue to review the investigative plan during subsequent case reviews. Case reviews will include an affirmative decision to continue or terminate the investigation.

i. Ensure that investigative steps include identification of causative factors that can be recorded as weaknesses or internal control issues requiring corrective action by management. This refers to material weaknesses within the command that led to the "loss, misappropriation, or other criminal act" to occur. An example would be a command's failure to establish procedures requiring the conduct of inventory(s) of pilferable equipment and/or classified material. NCIS' investigation looking into the loss of the item(s) would also document the lack of internal controls (i.e., an inventory process) as part of the material weakness of the command. This information must also be clearly identified as part of NCIS criminal investigation in order to insure the Director, NCIS, can accurately address the "material weakness" reporting requirements identified through NCIS investigative activities as stated in SECNAVINST 5200.35 series. It should be noted that few NCIS criminal investigations will surface material weaknesses, but those which do should be clearly identified.

j. Coordinate with appropriate Department of the Navy (DON) or other government officials if notable security, force protection, public health, or safety issues are raised.

k. Alert NCISHQ of investigations with potential seat of government/significant interest.

45-3.3. Investigative plans will be maintained in the case file, in addition to the Case Activity Record (CAR), during pendency of the case and may be destroyed one year after closure, along with case agent's notes, if the case file is no longer needed.

45-3.4. Case Reviews. The requirement for supervisors to conduct case reviews is well established within NCIS. Case reviews are among the most important functions performed by supervisors and must be conducted at least every 30 days. Supervisors may find it necessary to conduct case reviews more frequently, depending upon case complexity, performance issues, or for other reasons, but all open investigative and operational files are to be reviewed at least once every 30 days. Level I source files are to be reviewed at least semi-annually; level II and III source files are to be reviewed at least once every 30 days.

45-3.5. Case reviews must be meaningful and pragmatic in order to maximize supervisors' and case agents' time. The following specific case review guidance is established as NCIS policy:

a. Case reviews will be conducted face-to-face whenever possible. An exception may be made for agents in isolated assignments, for whom telephonic case reviews may be conducted. Face-to-face case reviews will be conducted during management visits and whenever feasible with agents assigned in isolated areas.

b. Supervisors will personally review case files, investigative plans and updates, and accompanying documentation.

c. Supervisors must be involved in establishing investigative strategy early on. In all investigations, supervisors and case agents will develop investigative plans within three working days.

d. Investigative progress, or lack thereof, and necessary investigative/operational steps will be the focus of each review.

e. Supervisors' case review must be documented and maintained separately from the case file. For further guidance, refer to 45-3.6. below.

f. Supervisors must ensure that case agents have a clear understanding of appropriate direction of the investigation/operation/source, investigative/operational actions required, and when actions should be accomplished. Both agents and supervisors will make note of issues discussed and specific action required.

g. Supervisors will document date(s) of supervisory review(s) and the specific supervisor who conducted each review in the CAR. The CAR will not address specific supervisory guidance, as that information will be confined to the supervisors' case review documentation.

h. Supervisors must follow-up to ensure direction/guidance provided during case reviews has been accomplished or is ongoing.

45-3.6. Case Review Documentation

a. The details of each case review must be documented by the supervisor in a written or electronic record of the supervisor's choosing. Case reviews must be dynamic and readily chronicle the supervisory direction/guidance and the planning, programming, verification, and evaluation phases of an investigation/operation. A clear understanding should exist between the supervisor and case agent regarding direction of the investigation/operation, future actions required, and timeframe for these actions to be completed. Case review documentation will include a record of relevant case information, in chronological order, so the reviewer knows exactly what has been completed during the course of an investigation, as well as what has not been accomplished since the last case review. By following up on deadlines, case review sessions serve as excellent opportunities to discuss investigative strategies and accurately track employee productivity. SSAs may establish their own tailored case review documentation, as long as it complies with the intent listed above. The Case Review Record (CRR) and CRR Continuation Sheet, Appendix 1 and Appendix 2 respectively, are offered as examples for capturing case review documentation. These forms are available for download and electronic completion via the NCISnet (Download, Forms). For a completed sample CRR, see Appendix 3.

b. All case review documentation must be maintained separately from the case file and will be the document of record for inspection purposes. The case review documents will be destroyed with locally held copies of case files (in most cases, one year after closing). Case review documents are not discoverable. If you receive a discovery request for any case review documents, contact NCISHQ Legal Division (Code 00L) for guidance. Under Rule of Courts Martial (R.C.M. 914) and the Jencks Act, case review documents as well as agent case notes, may be ordered by the court to be produced for the defense counsel after the agent or reviewing supervisor testifies. For additional information on the Jencks Act, see NCIS-3, Chapter 6 (Investigative Theory and Procedures).

45-4. CASE MANAGEMENT

a. Multiple six-panel divider folders will be used for all control cases, except threat assessments and other one-time documentation. Six-panel folders allow more specific filing of investigative documents (evidence custody documents, investigative notes, etc.), and easier review and retrieval of those documents.

b. Single sheet file folders may be used for leads, sources, ROI (INFO) and single (i.e., one-time) ROI (CLOSED) reports.

c. All case files (field copies) will be destroyed one year after case closure, unless the case is placed into extended retention.

d. Lead cases (ROI (ACTION)) will be maintained by the office responding to lead tasking for 90 days after completion of tasking.

45-4.1. Standard Case File Setup. Case files for all control cases will be divided into separate sections containing the following information or documentation:

Section 1 – Administrative Forms (front cover – inside)
Case Activity Record (CAR)
Copy of Evidence Custody Document (ECD)
Case Tracking and File Management Form (CTFMF)

Section 2 –Administrative Investigative Forms
Records Information Management System (RIMS) Cover Sheet (Closed cases only)
Investigative Plan (IP)
Fingerprint Card, Green Fingerprint Form
Victim/Witness Contact Log (VWCL)
Suspect Photographs

Section 3 – Consolidated Law Enforcement Operations Center (CLEOC) Documents
CLEOC – GEN CRIM cases only (Print and include all updates)

Section 4 – Case Supporting Documentation
Investigative Action ((IA) not yet attached to an ROI), Exhibits, and Enclosures

Section 5 – Standard System Document (SSD)
SSDs in chronological order (ROI (OPEN) on the bottom, ROI (CLOSED) on top)

Section 6 – Agent Case Notes

45-4.2. Section 1: Administrative Forms

a. The Case Activity Record (CAR), (Appendix 4), is found on the NCISnet under Downloads, Forms, and lists all activities relating to a case in chronological order (i.e., phone calls, command notifications, interviews, interrogations, record checks, guidance/taskings requested by prosecutive authority, etc.). Supervisors annotate and date CARs to reflect that case review has been completed. Specific details of case reviews will be confined in the supervisor's case review documents.

b. The Evidence Custody Document (ECD) is a multi-carbon copy form used to track evidence collected during the pendency of an investigation, and to ensure that chain of custody has been maintained. The original ECD is maintained with the evidence, the second copy is retained in an ECD binder controlled by the evidence custodian, and the third copy is filed in Section 1 of the case file.

c. The Case Tracking and File Management Form (CTFMF), (Appendix 5), is found on the NCISnet under Downloads, Forms, and is the only authorized form for case tracking. CTFMFs are used to identify administrative and investigative processes used during the conduct of an investigation or operation.

45-4.3. Section 2: Administrative Investigative Forms

a. When a case is closed, the Records Information Management System (RIMS) Cover Sheet is completed electronically and printed by the professional administrative staff, signed by the SSA, and placed in Section 2, as the top document. There are two separate cover sheets, one for counterintelligence/counterterrorism records and one for law enforcement records. These cover sheets must be generated electronically through RIMS. To access RIMS on the NCISnet home page, click on Web Applications then click on the RIMS link. Once you log into RIMS, click on the appropriate cover page link (Counterintelligence/Counterterrorism Records or Law Enforcement Records) under the Create Cover Pages section. For instructions on creating cover pages, refer to the RIMS User Guide (Appendix 6). The RIMS User Guide can also be found on the NCISnet under Guidelines & Reference, Manuals and User Guides. Additional RIMS cover sheets, utilized as needed, are the Cross Reference Sheet (Appendix 7) and Supplemental Coversheet (Appendix 8); these sheets can also be found on the NCISnet under Downloads, Forms, Case Management Forms. Cross Reference Sheets are used to document material that cannot be currently imaged. Additional guidance to assist with identifying case record series and Defense Central Index of Investigations (DCII) indexing code information is located as Appendix 9. Such RIMS guidance is also available on the Administrative Services intranet website, Tools page, then under Closed Case Files Guidance.

b. The Investigative Plan (IP) is formulated by the agent, along with the SSA, within three working days of case initiation. The Investigative Plan is a living document that will be updated and reviewed during the pendency of the investigation.

c. The Victim/Witness Contact Log (VWCL), (Appendix 11), is found on the NCISnet (Downloads, Forms, Case Management Forms), and is used to document contact information for witnesses related to the investigation.

45-4.4. Section 3: Consolidated Law Enforcement Operations Center (CLEOC) Documents.

CLEOC is a web-enabled reporting program that is used by the DON law enforcement community (NCIS, U.S. Navy, and U.S. Marine Corps) for consolidated analysis and reporting of criminal activity. CLEOC enables the DON law enforcement community to record investigative data and subject/victim information for case categories 4, 6, 7, and 8. It also serves to input witness identities and vehicles associated with an investigation. A printed copy of the initial entry into CLEOC, as well as all updates, will be included within Section 3 of the case file.

45-4.5. Section 4: Case Supporting Documentation

Investigative actions (IAs) are investigative support documents such as inventories, police reports, results of interviews, etc. IAs maintained in this section are only those collected subsequent to submission of the last ROI (INTERIM). These IAs will become exhibits to future ROIs.

45-4.6. Section 5: Standard System Document (SSD)

All SSD documentation will be filed in chronological order, with the most recent document on top. Documents may be printed from K-NET provided that the "Print with Warning Banner" option is used.

45-4.7. Section 6: Agent Case Notes

Case notes will be annotated to include the case agent's initials, location of interview/action, date and time of the interview/action, the case control number (CCN), and the NI title. Case note pages will be numbered consecutively (i.e., 1 of --) and be secured in an Investigative Notes (NCIS Form 025) envelope.

45-4.8. Closed Case Submission

a. Administrative Services Department, Records Management Branch (RMB) (Code 11C1) is responsible for storage and management of closed case records. Routine closed case files should be addressed to NCISHQ, Files Section, Code 11C12, via United States Postal Service (USPS) registered mail or equivalent means.

b. Director's Special Interest (DSI) and Special Interest (SI) case files will be sent via FedEx or UPS directly to applicable operational codes. Additional investigative/operational case file exceptions for mailing are noted below:

(1) 7H death and 7F fugitive cases should be sent to the Criminal Investigations Department (Code 23B).

(2) 5T investigative case files and XXCT operational files will be sent directly to Code 21. If the case file contains classified material, it will be stored, handled and mailed in accordance with security guidelines.

(3) 3C investigative/operational case files will be sent to Office of Special Projects (OSP) (Code 22E). XXCE case files will be sent directly to the Counterintelligence Directorate (Code 22). If the case file contains classified material, it will be stored, handled and mailed in accordance with security guidelines.

c. In addition to a thorough administrative quality control check, a detailed closed case file review must be conducted by the SSA to ensure all required and logical investigative steps have been completed and appropriately documented. This is to be done prior to sending the case file to NCISHQ in accordance with case management guidance for routine closed case file submission to RMB. For additional guidelines on closed case submission, see NCIS-1, Chapter 25.1 (SSD Report Writing).

45-4.9. Field Office Management Visits. SACs are responsible for ensuring meaningful case reviews are being conducted regularly by subordinate supervisors. Senior field office managers should focus significant attention on case management during self-inspections and each management visit to subordinate elements. Protocols for field office management visits and reporting requirements can be found on the Inspector General's website on NCISnet.

45-5. EXECUTIVE ASSISTANT DIRECTOR (EAD) RESPONSIBILITIES

Executive Assistant Directors (EADs) for Atlantic (LANT) and Pacific (PAC) are responsible for providing oversight to ensure proper conduct, timeliness, and quality of administrative, investigative and operational programs in their subordinate offices. The EAD for Global Operations is responsible for similar monitoring of the Office of Strategic Support and OSP. Guidance for conducting field office management visits is found in NCIS-1, Chapter 5 (Inspector General Matters).

45-6. HEADQUARTERS RESPONSIBILITIES

45-6.1. NCISHQ directorate managers are responsible for providing oversight of related field activities. Operational Directorate DADs will:

a. Designate and monitor all DSI investigations.

b. Ensure seat of government (SOG) notification on significant investigations as required by SECNAVINST 5500.30F, Section 811 of the Intelligence Authorization Act of 1995, intelligence community directives, memorandums of understanding, and other directives.

c. Task field offices for investigative, operational, or source status on DSI cases and those cases for which timely reporting has not been received in accordance with NCIS-1, Chapter 25.1 (SSD Report Writing).

d. Monitor and review all source reporting for validation and testing. The Intelligence and Information Sharing Directorate (Code 25) will maintain administrative oversight of all field office source reporting.

e. Disseminate lessons learned and policy guidance to field offices based upon trends, best business practices, and shortcomings identified during the oversight process.

45-6.2. During field office inspections, the NCIS Inspector General will scrutinize the case review processes, involvement of supervisors in providing oversight and direction during the conduct of investigations, and compliance with timeliness standards.

45-6.3. A representative from the Financial Management and Planning Directorate (Code 14) will participate in IG inspections to help monitor and report on field office performance plan implementation procedures.

45-7. DIRECTOR'S SPECIAL INTEREST (DSI) AND SPECIAL INTEREST (SI) INVESTIGATIONS

The DSI category is reserved for the most significant cases. Investigative direction, accountability, and responsibility for all DSI cases is assigned to NCISHQ. The role of NCISHQ in DSI cases is envisioned to be a cooperative partnership with field components to enhance investigative focus and timeliness of those investigations identified by the Director and Executive Staff as having clear Department of Defense (DoD)/DON-wide or NCIS-wide implications or other significant SOG level interest. Full authority and responsibility for SI cases and all other routine investigative activity will remain under the stewardship of field EADs. This policy standardizes DSI and SI case management and reporting protocols for criminal, fraud, counterintelligence, and counterterrorism investigations. Appendix 12 provides a summary of criteria for identifying DSI and SI investigations.

45-7.1. DSI Investigations

a. DSI designated cases will be limited to those matters having clear DoD/DON-wide or NCIS-wide implications. The Director reserves discretion to declare any NCIS investigative activity or other sensitive matter DSI if circumstances warrant such action.

b. An investigation may only be declared DSI by NCISHQ.

c. Field components will immediately notify the cognizant NCISHQ directorate of initiation of investigations involving any of the criteria summarized in Appendix 12. Under no circumstances will notification be delayed beyond 24 hours. Notifications will be made by the quickest (and secure if classified) method available.

d. NCISHQ will determine if the case warrants immediate DSI status or may recommend SI status to see how the case develops.

e. NCISHQ will be the lead investigative partner in all aspects of a DSI investigation, and retains authority to direct/task investigative coverage. In the event of variances in investigative guidance between NCISHQ and field components, the matter will be referred to the SAC/DAD for resolution.

f. Once NCISHQ declares an investigation DSI, the field component will communicate with NCISHQ within 24 hours to devise a preliminary investigative plan of action. Thereafter, an initial IP must be submitted within 72 hours. NCISHQ can assist in developing the IP, and when necessary, direct or otherwise provide additional resources to expedite the process. The IP is envisioned to be a cooperative effort between the field component and NCISHQ. However, the field component will execute the IP and maintain case management and supervisory oversight of field work.

g. Once an IP has been formulated, the field component will coordinate all investigative actions with NCISHQ. All investigative actions will be documented in the case file.

h. Unless NCISHQ directs Priority I reporting requirements as delineated in NCIS-1, Chapter 25.1, an initial ROI (INTERIM) reporting all investigative actions to date will be submitted within 15 business days of case initiation with a subsequent ROI (INTERIM) with exhibits every 30 calendar days. Weekly updates will be provided to NCISHQ in a manner agreed upon between the field component and NCISHQ. All investigative actions and other related operational case activity must be reported in applicable NCIS investigative reporting format consistent with the appropriate classification level.

i. Only NCISHQ may downgrade DSI status in the event circumstances warrant such action prior to completion of an investigation.

j. Specific investigative and reporting protocols for occasions when an agency other than NCIS is the lead agency of a major investigation/operation will be addressed on a case-by-case basis. Regardless, the NCISHQ notification requirements for initiation of DSI/SI cases remain the same.

45-7.2. SI Investigations

a. Cases not designated DSI, which nonetheless meet the criteria summarized in Appendix 12, but that do not appear to have DoD/DON-wide or NCIS-wide implications, shall be designated as an SI investigation. Any other sensitive issues involving individuals or circumstances that would potentially require senior leadership briefing by NCISHQ shall also be designated SI.

b. An investigation may be declared SI by NCISHQ or EADLANT/EADPAC.

c. Field components will ensure the ROI (OPEN) summarizing the circumstances of the investigation is transmitted to NCISHQ/EADLANT/EADPAC within 72 hours of case initiation.

d. EADLANT/EADPAC, jointly with the field component, will establish a timetable for development and submission of an IP. Field components may request guidance or other assistance from NCISHQ; however, the IP and concomitant investigative actions will remain a field component product.

e. Unless NCISHQ or EADLANT/EADPAC directs Priority I reporting requirements as delineated in NCIS-1, Chapter 25.1, an initial ROI (INTERIM) reporting all investigative actions to date will be submitted within 30 calendar days of case initiation with a subsequent ROI (INTERIM) every 30 calendar days. Bi-weekly updates will be provided to NCISHQ in a manner agreed upon between the field component and NCISHQ.

f. All case related actions and other related case activity must be reported in the applicable NCIS investigative reporting format consistent with the appropriate classification level.

g. Upon obtaining concurrence from NCISHQ/EADLANT/EADPAC, field office SACs may downgrade SI status if circumstances warrant such action prior to completion of the investigation. NCISHQ/EADLANT/EADPAC reserves the prerogative to reinstitute SI status of a particular investigation if deemed necessary.

h. It is the responsibility of EADLANT/EADPAC to establish a system to identify and monitor any investigative matters under their purview that they consider to be cases of interest and to ensure that NCISHQ is promptly alerted to any issues that could potentially require SOG level advisements or otherwise be elevated to SI or DSI status.

i. Accountability and responsibility for SI investigations will remain with EADLANT/ EADPAC.

j. Specific investigative and reporting protocols for occasions when an agency other than NCIS is the lead agency of a major investigation/operation will be addressed on a case-by-case basis. Regardless, the NCISHQ notification requirements for initiation of DSI/SI cases remain the same.

45-7.3. Other Timely Notifications

a. There will be other cases of interest not falling under the DSI/SI reporting requirements that necessitate reporting of definitive information to NCISHQ in a timely manner. These notifications will provide the Director/Deputy Director with timely and accurate information for briefings of senior DoD/DON officials. A complete listing of those types of cases can not be reasonably constructed; however, guided by experience and common sense, field component leaders must recognize the kinds of issues that generate senior level DoD/DON interest or those that may potentially receive media attention. These issues may include, but not limited to; politically sensitive issues; potentially embarrassing situations involving DoD/DON persons; incidents occurring in foreign areas that could affect host country relations or any other incidents of notoriety in which NCIS is investigating, providing assistance or otherwise actively involved.

b. The initial notification will be made to the Multiple Threat Alert Center (MTAC) (Code 25C) via voice communication, keeping in mind the security classification of the information, detailing what facts are known and what potentially pertinent information is not known. The MTAC will provide a follow-up e-mail with written details of the voice report and will provide e-mail updates until the field can directly engage with the cognizant operational code. Distribution of the follow-up e-mail correspondence will include the DDO, DD management staff, relevant program and operational EADs, geographic EADs, NCIS public affairs officer (PAO) and affected field office SAC(s). The necessity for subsequent periodic updates will be determined on a case-by-case basis and in a manner agreed upon between the field component and NCISHQ.

Pages 1069 through 1081 redacted for the following reasons:
- -
(b)(7)(E)

CHAPTER 46
TITLE: RECRUITMENT, SCREENING AND SELECTION OF SPECIAL AGENTS
POC: CODE 10A
DATE: DEC 06

APPENDICES:

APPENDIX (A): SPECIAL AGENT APPLICATION PRE-EMPLOYMENT SUITABILITY INVESTIGATION

POLICY DOCUMENT:

APPENDIX (B): Gen Admin 11C-0044 of 29DEC2011 released NCIS Policy Document No. 11-26 Administrative (Special Agent Periodic Physical Examination Requirements) Policy Document 11-26 contains revised or new policy that has not been incorporated into this chapter and should be reviewed in its entirety.

46-1. INTRODUCTION

This chapter covers the recruitment, screening, testing, and selection of candidates for Special Agent (SA), GS-1811 positions with the Naval Criminal Investigative Service.

46-2. BACKGROUND

a. Scope. The SA career field includes all civilian employees of NCIS covered by the criminal investigator series, GS-1811. The mission of the SA is to prevent terrorism and related hostile acts against DON forces and installations; protect against the compromise of operations, information and systems that would cause an unacceptable risk to DON personnel and strategic assets; and reduce criminal activity and mitigate its impact on Navy and Marine Corps operational readiness. NCIS SAs operate under a strong, centralized and structured program to guide career development through judicious assignment practices and professional training programs on the national and local level.

b. Mobility. Selective movement of SAs provides exposure to various investigative and counterintelligence elements. Mobility is necessary to develop SAs and make them fully aware of the overall DON mission and enable them to respond to operational requirements rapidly and effectively. Transfer of SAs to the various field offices and NCISHQ for purposes of career development is not only highly desirable, it is essential to the accomplishment of the NCIS worldwide mission. Such movements provide opportunity for breadth of experience, knowledge, improved confidence, adaptability and effectively promote professional development. The reassignment provisions of the appropriate government-wide regulations must be universally applied to all SAs at all levels worldwide.

c. Investigative and Technical Specialties. Four investigative specialties (Generalist, Fraud, Counter Terrorism, and Counterintelligence) and four technical specialties (Technical Services, Cyber, Forensics and Polygraph) have evolved within NCIS. Each of the specialties includes a management commitment to equal career opportunities, challenging and rewarding work, equal pay for work of equal difficulty and complexity, and the opportunity for development of management skills and abilities.

46-3. SPECIAL AGENT QUALIFICATION REQUIREMENTS

Applicants for SA positions will be given equal consideration without regard to race, religion, color, sex or national origin. Initial screening will be conducted against the following criteria:

a. Driver's License. All applicants must possess a valid motor vehicle operator's license.

b. Minimum Entry Age. The minimum age for SA positions is 21 years.

c. Maximum Entry Age.

(1) The maximum date for entry into a SA position is the date preceding the 37th birthday (Public Law 101-509, Section 409).

(2) Applications must be submitted before the applicant reaches 36 years and 6 months of age to accommodate hiring by the applicant's 37th birthday.

(3) In limited cases, exceptions to this requirement may be available for applicants seeking to transfer from a covered (1811) position or for individuals with previous applicable covered service.

(4) In extremely rare circumstances, a waiver to the age limit may be considered. Age waivers must be approved by the Secretary of the Navy and shall be based only on the compelling interests of the agency. The specific individual for whom a waiver is requested must present special or unique skills not otherwise available.

d. Citizenship. An applicant must be a United States citizen either native born or naturalized. If an applicant possesses dual citizenship, non-U.S. citizenship must be renounced prior to initiation of applicant processing. Proof of renouncement must be included in the application package. U.S. citizenship is required of each member of the applicant's immediate family, which includes spouse, cohabitant, parents, brothers, sisters and children. Normally, citizenship waivers will not be granted for any applicants or members of their immediate family, however, waivers are available for spouses. In those rare cases where there is a demonstrated compelling need, a written request for a waiver may be submitted to DIRNCIS via the Deputy Assistant Director for Personnel Operations and Services.

e. Personal Characteristics.

(1) Good character and reputation.

(2) Unquestioned loyalty, patriotism and integrity.

(3) Good judgment; a pronounced sense of personal responsibility.

(4) A high degree of individual initiative and dependability.

(5) Ability to deal tactfully and effectively with others.

(6) Well-developed powers of observation and comprehension.

(7) Demonstrated ability in oral and written communication.

(8) Good personal appearance and bearing.

f. Education. Applicants must possess a 4-year degree from a college or university accredited by one of the regional or national institutional associations recognized by the United States Secretary of Education.

g. Physical Requirements. Applicants must be in excellent physical condition and meet the following minimum requirements:

(1) Normal hearing (must be able to pass an audiometer test). Hearing loss exceeding a 25-decibel average in either ear in the conversational and speech range (500, 1000, 2000 cycles) would be disqualifying.

(2) Corrected vision of 20/20 in one eye, and 20/30 in the other eye. There is no uncorrected vision requirement. An applicant who has undergone radial keratotomy, photorefractive radial keratotomy or laser surgery cannot apply until 1 year following the surgery and must submit a letter from the ophthalmologist concerning the prognosis of the procedure.

(3) Applicants are required to pass a red/green color vision test.

(4) Applicants must be capable of strenuous physical exertion (see paragraph 46-5.d).

46-4. RECRUITMENT AND SCREENING

a. Field Office Responsibility. Each NCIS field office is responsible for conducting an active recruitment program to ensure that a pool of qualified applicants for SA positions is available to fill anticipated vacancies. It is essential that recruitment activities be conducted to ensure a diverse pool of candidates with a wide variety of background and experience. At times it may be necessary to increase the pace of recruitment and processing of agent applicants to meet hiring goals. In these cases, it is imperative NCIS continue to recruit and process only the most highly qualified applicants and not lower standards in an effort to meet peak recruitment needs. Each field office will submit an annual recruiting plan to Code 10A for approval. Recruitment initiatives/events must be approved by NCISHQ, Code 10A3, in advance in order to obtain NCISHQ funding.

b. Headquarters Responsibility. The composition of the SA corps is critical to the success of the organization. NCISHQ, Code 10A will provide guidance to the field regarding long-term and annual recruitment goals and strategies and will provide funding for approved

recruitment initiatives/events. Employment and advancement decisions affecting the SA corps are the responsibility of the Assistant Director for Human Resources and the Deputy Assistant Director, Personnel Operations and Services. Field office representatives must not make commitments of employment or make comments concerning employment, duty stations, initial grade level, etc. to any potential candidate. A potentially successful applicant should be advised that final employment decisions are based on a comparison of his/her qualifications with those of other applicants. The keen nationwide competition for the limited number of SA positions makes it possible for an applicant to meet all of the required qualifications and not be selected. The field office is responsible for keeping the applicant informed of his/her status during processing.

c. Recruitment, Screening and Testing of Relatives. The rules governing employment of relatives are delineated in 5 CFR Part 310. In compliance with this Part, a NCIS supervisor or manager shall not:

(1) Advocate one of his/her relatives for appointment, employment, promotion, or advancement to a position within NCIS over which he/she exercises jurisdiction or control.

(2) Appoint, employ, promote, or advance one of his/her relatives to a position within NCIS over which he/she exercises jurisdiction or control.

(3) Appoint, employ, promote, or advance the relative of another NCIS manager if the manager has advocated the appointment, employment, promotion, or advancement of that relative.

(4) When relatives of current NCIS employees are considered for employment, they will be screened, tested, and processed in accordance with the policy contained in Part 310, Section 310-103. Screening and testing will not be conducted in or by the organizational element where the current NCIS employee is assigned.

d. Initial Application Process. Candidates must apply online through the automated system accessible either through the NCIS website (http://www.ncis.navy.mil) or USAJOBS (http://www.usajobs.opm.gov/). If the applicant meets basic eligibility and the application is accepted for further processing, it is forwarded to the appropriate field office for prescreening, including administration of appropriate tests. Applicants not meeting basic eligibility requirements and those not recommended for testing will be notified in writing and/or via email by NCISHQ Code 10A.

e. Testing.

(1) The first formal step in the processing of an agent applicant is the SA Applicant Test Battery. All applicants who were deemed suitable for further processing will be afforded the opportunity to take the test battery. The test battery, used primarily as a pre-screening tool, measures the applicant's ability by use of a biographical inventory, a reading comprehension exercise and a psychological inventory.

(2) NCISHQ will manage test content and procedures. Field offices will administer tests to potential candidates. The test is scored on a pass/fail basis. The designated field office representative is responsible for scoring tests they administer. Scored test batteries are retained in the field office; Code 10A should be notified of the results via e-mail as soon as scoring is completed.

(3) Applicants not achieving a qualifying score will be notified in writing of their non-selection. Applicants may take the test up to a total of two times after reapplying on line as described in subparagraph d above.

f. Pre-screen Interview.

(1) The second formal step in the processing of an agent applicant is a prescreen interview conducted by an experienced SA at or above the GS-13 level. The interview should be conducted utilizing the format and detailed guidance found in the Prescreen Package. The purpose of this interview is to determine whether the applicant possesses the general requirements/qualifications enumerated in subchapter 1, to determine the individual's motivation for seeking employment with NCIS, and to determine his/her availability for employment.

(2) Applicants will be asked whether they have previously applied for a position with NCIS or any federal law enforcement or intelligence agency, and if so, the circumstances, location and results of the application. If an applicant was previously screened for a position with NCIS, Code 10A should be contacted to determine the results of the screening.

(3) The interviewer will provide the applicant with the Civilian Mobility/Transfer Stipulation Agreement form and the individual will be requested to list three areas of preference in the order desired. The applicant will also be asked to read and sign the form signifying his/her understanding of the transfer policy contained in subchapter 7 of this policy. The signed form will be returned to Code 10A along with the Prescreen Worksheet and accompanying documentation.

b7E

(5) If, following the prescreen interview, the applicant is recommended for further processing, the interviewer will contact the applicant's current employer to ascertain his/her suitability for the position. The interviewer will complete the Employment Verification Form for each contact.

(6) If, following the prescreen interview, the interviewer determines the applicant does not merit further processing, Code 10A will be advised and, if in agreement, will notify the applicant of non-selection.

(7) The importance of the prescreen interview cannot be overemphasized. This stage of the screening process should be used to eliminate all unqualified or marginal applicants, thereby eliminating the need to conduct a screening board.

g. Screening Board. Applicants who successfully complete the pre-screen interview will be scheduled for a screening board interview.

(1) Prior to the screening board, the applicant will be asked to complete a SF 86 (Personnel Security Questionnaire/Background Investigation.) The applicant should be advised to complete the forms in accordance with the accompanying instructions and bring the completed forms when reporting for the screening board. The forms must be typed. The applicant should be cautioned that a part of the screening process is his/her ability to complete the forms accurately and in accordance with the instructions.

(2) The Screening Board will be comprised of three civilian SAs. In extreme circumstances, a Screening Board consisting of only one or two SAs may be held, however, prior approval of the Deputy Assistant Director for Personnel Operations and Services must be obtained. The chair of the Screening Board will be a GS-14 SA or above with the remainder of the board being comprised of senior GS-13 SAs.

(3) Prior to questioning, the applicant will be informed of the requirements of the Privacy Act (5 U.S.C. 552a(e)(3)) and provided a copy of the appropriate Privacy Act Statement (PAS). Each Screening Board Report (SBR) will contain an entry indicating compliance with this requirement. A copy of the signed Privacy Act Statement will be forwarded to NCISHQ Code 10A as part of the SBR.

(4) The Screening Board interview will be used to determine the applicant's:

b7E

(5) It is recommended that individual Screening Board members be assigned specific subject areas for questioning to include those enumerated above. This will allow for more in-depth questioning and ensure none of the areas are overlooked or covered only superficially.

(6) During the interview, the applicant will be provided unclassified information to facilitate understanding of conditions under which he/she would be working if employed as a SA. These matters should include but not be limited to the following:

(a) Newly hired NCIS employees are required to bear all expenses of travel, transportation and movement of household effects to the first duty station.

(b) NCIS employees may be transferred within or outside the continental limits of the United States at the convenience of the government and in accordance with the Mobility Program (NCIS-1, Chapter 13). During a 20-year career, the average SA can expect a number of such moves.

(c) NCIS SAs may reasonably expect to serve at least one tour in the Special Agent Afloat Program or a temporary deployment in support of overseas missions, often times in hostile environs.

(d) Investigative duty is not confined to a normal 8-hour working day. Hours of work outside the normal workday are usually compensated through Law Enforcement Availability Pay (LEAP) calculated as a percentage of basic pay.

(e) Initial and continuing physical fitness is **mandatory** for the performance of investigative duties and physical examinations will be required on a continuous basis.

(f) Shortly after appointment, NCIS SAs, as a condition of employment, must qualify in the use of small arms and must re-qualify quarterly thereafter. SAs are also required to maintain continuing proficiency in apprehension techniques and unarmed self-defense.

(g) While employed by NCIS, SAs will be required to submit to random urinalysis testing for illegal drugs. Failure to pass the drug test can result in termination of employment.

(h) Successful completion of the Basic Agent Course of instruction at the Federal Law Enforcement Training Center (FLETC) is a condition of employment.

(7) If at any stage of the screening process, the Board determines that the applicant is not qualified, further processing will cease. A SBR recommending non-selection must be forwarded to NCISHQ Code 10A.

(8) An applicant who is not recommended by a Screening Board will be advised of his/her non-selection in writing by Code 10A. The applicant may not reapply for one year following the date of the non-selection letter.

(9) Detailed guidance, instructions and samples, including a list of required documents, may be found in the Screening Board Report.

(10) Finalization of the Screening Process. Upon receipt of the SBR and based on the competitiveness of the candidate, the recommendation of the Screening Board, and anticipated staffing requirements, Code 10A will determine whether to continue, cease or defer further processing of the application.

h. Pre-employment Inquiries will be conducted in accordance with Appendix A.

i. Re-employment of a former NCIS Special Agent. When a former NCIS Special Agent applies for re-employment, the following procedures apply:

(1) A current NCIS-0001/NCIS-0002 and OF-612 or resume will be submitted.

(2) A detailed interview will be conducted by a NCIS supervisory SA, GS-13, or SA manager, GS-14 or above. The results will be provided by memorandum to Code 10A via the chain of command, and will contain comments concerning the applicant's motivation for reemployment and other pertinent observations.

(3) The applicant's previous NCIS dossier will be recovered from the archived files.

(4) All documents will be reviewed by Code 10A. Applicants determined to be free from derogatory or questionable information will be referred for initiation of a pre-employment background investigation. The background inquiries will cover the span from the time of the applicant's termination of employment with NCIS to the time of application. This inquiry (2A) will include local agency checks, credit checks, and employment inquiries at a minimum.

(5) The completed applicant package will be provided to the Deputy Assistant Director for Personnel Operations and Services, who will make the final determination on reemployment eligibility.

j. Priority Placement Program. In conformance with the Department of Defense Program for the Stability of Civilian Employment, prior to the final selection of a candidate for a position of SA, NCISHQ Code 10A will contact the Human Resources Service Center Northwest, who will check the stopper list for qualified candidates for the position of SA (1811).

k. File Retention. The following file retention standards will apply to all agent applications.

(1) All documents received from the applicant will be retained by NCISHQ Code 10A for a 3-month period.

(2) For applicants who are screened but who are not recommended by the Screening Board for further processing, pertinent documents such as Personal Qualifications Statement (Official Form 612), Application for NCIS Employment (NCIS-0001), Statement of Personal History (SF Form 86), birth certificate, college transcripts, naturalization certificate, photographs, etc., will be maintained with the file by Code 10A.

(3) Screening Board Reports and directly related material may be exempt from disclosure pursuant to 5 U.S.C. 552a(k)(6), but, other administrative paperwork associated with the application is not exempt. The field office shall retain a copy of the SBR for 90 days. A copy of the screening board package will be forwarded to NCISHQ (Code 10A) for retention.

(4) When an applicant is recommended by the Screening Board for further processing, the field office forwards the SBR along with required documentation to Code 10A. The field office shall retain a copy of the SBR for no longer than one year. When an applicant is hired, Code 10A will notify the field office to destroy the file.

(5) NCISRAs will not retain SBRs under any circumstances. When it is determined by NCISHQ that an applicant is no longer to be considered for employment, Code 10A will notify the applicant of non-selection. A copy of the non-selection letter will be filed in the applicant's dossier with the original SBR, pre-employment inquiries if initiated, and other pertinent material and retained for a period of five years.

(6) Application files on successful candidates will be considered active for a period of 1 year. If employment is not offered during this period, the applicant will be contacted by Code 10A regarding continued interest in employment with NCIS. If still interested, they will be considered for employment for a second year. Files on successful candidates who were not offered employment during the 1- or 2-year active status period will be retained at NCISHQ for a period of 1 year beyond the application expiration date, and then destroyed.

(7) Application files on candidates who have been rejected for cause will be retained at NCISHQ for a period of 5 years. This file material will be available should the rejected candidate make subsequent application to any NCIS component.

46-5. PHYSICAL, MEDICAL AND FITNESS QUALIFICATIONS

a. General Requirements. The physical, medical and fitness requirements of the Special Agent Career Program include a pre-employment physical, periodic physical examinations throughout the career, aperiodic drug testing, and regular physical fitness training and testing.

b. Pre-Employment Physical.

(1) A pre-employment physical examination will be conducted as part of the screening process. Results of examinations become part of the background investigation file and, along with other background information, will be used to formulate selection decisions. Field office personnel responsible for processing the application will make arrangements for the

required physical examination. The examination should be administered by a Navy Medical Officer or, if unavailable, by another Federal Medical Officer.

(2) When the completed report of medical examination is returned to the appropriate NCIS field office, it must be reviewed to ensure that it is complete and the forms properly filled out and signed by the examining physician. Before an applicant may be employed, he/she must be certified as being physically capable of performing arduous physical duties without hazard to him/herself or others.

(3) The examining physician must provide information on any existing physical handicap(s). The physical demands of the SA position must be fully explained to the medical officer, particularly the necessity for SAs to operate motor vehicles, use firearms and react appropriately to unexpected emergency situations, including temporary or sustained assignment to overseas areas where medical facilities meeting normal U.S. standards may not be available.

c. Medical Restrictions. The following requirements regarding specific diseases and defects will be followed, using as a general standard the objective that the individual must be physically capable of performing efficiently the duties of the position without hazard to him or herself or others (see 5 Code of Federal Regulations (CFR) 339 and 5 CFR 842):

(1) Tuberculosis. Under no condition may persons with active tuberculosis be employed as a SA. Persons with arrested cases of tuberculosis may be employed if the condition is shown by medical evidence to be arrested and the general health of the individual is good. For arduous duty positions where there are unusual hazards, the individual may be approved by a Federal Medical Officer on the basis of the period of arrest and the history and extent of the disease. The case must be proven to be that of a minimal tuberculosis lesion that has been arrested for at least five years.

(2) Diabetes. 5 CFR 339 does not preclude the employment of diabetics provided their condition is controlled. Persons who have their condition under control by diet, oral medication, or 25 units or less of insulin per day; possess full capacity in the required environmental and functional factors; and if they meet the following criteria may be considered physically qualified to perform the duties of a SA position:

(a) No insulin reaction, diabetic coma, or serious side effects within the past 2 years.

(b) No significant change in the amount of insulin required during the past two years.

(c) A good work record or other proof of stability of the diabetic condition.

(3) Peptic Ulcer. Prospective employees with a history of peptic ulcers are not normally accepted for arduous duty positions unless in the opinion of a Federal Medical Officer the ulcer has been healed.

(4) Blood Pressure. Maximum: Systolic 150, diastolic 90. These standards may be applied where all other evidence relating to circulatory system is favorable (that is, in uncomplicated cases of high blood pressure). In the case of initial employment, waivers of the maximum and minimum blood pressure readings will not be granted. Cases exceeding this reading must be referred to a Federal Medical Officer for an employability opinion in keeping with Section 13-3.5.

(5) Other Diseases or Physical Defects. When review of medical evidence indicates the existence or history of one of the following diseases or physical defects, the case must be referred to a Federal Medical Officer for an employability opinion under Section 13-3-5.

(a) Communicable diseases such as: Syphilis, Acquired Immune Deficiency Syndrome (AIDS), gonorrhea, Chlamydia or herpes.

(b) Mental Disease.

(c) Epilepsy.

(d) Organic heart disease.

(e) Severe crippling condition.

d. Physical Capability. The general requirement is that the applicant must be physically capable of performing efficiently the duties of the position without hazard to him or herself or others. In the event a medical officer recommends an applicant as physically qualified even though all the above requirements have not been met, the Deputy Assistant Director for Personnel Operations and Services will make a determination if further processing of the applicant is warranted.

e. Periodic Physical Examinations. Physical examinations of all SAs will be conducted as indicated below and certification made that the SA is physically capable of performing arduous physical duties without hazard to the SA or others. Examinations should be administered by a Navy medical officer or if unavailable, by another Federal medical officer.

(1) The physical will be conducted within 30 days before or after a SA's birthday.

(2) The Certificate of Fitness For Duty will be forwarded to Code 10A within 30 days of completion of the physical. Due to Health Information Privacy Act (HIPA) regulations, the physical and supporting documentation will be maintained by the facility conducting the examination. For new hires, the pre-employment physical will take the place of a periodic physical for the first calendar year of employment.

(3) Physical exams will be required for SAs as follows:

(a) Entry/Applicant

(b) At Age 24, 27, 30, 33, 36, 38, 40

(c) Every year after age forty

(4) Field Operations Support Officers (FOSOs) are to ensure physical examinations are conducted on all SA personnel as required, and to ensure all SAs meet all the physical requirements covered in this subchapter. SF-600 Record of Medical Care contains the Physical Exam Matrix for Naval Criminal Investigative Service SAs.

(5) Physical requirements for incumbent civilian SAs are the same as those described for pre-employment physicals (see Sections 13-3.2 through 13-3.4).

f. Fitness for Duty. A fitness for duty physical under 5 CFR 339 may be ordered in any case where a SA is unable to perform the arduous and physically demanding duties of the position. A first-level supervisor will obtain concurrence of the next supervisory level prior to advising the employee of the requirement to report for a fitness for duty physical.

(1) If a medical officer recommends a SA as physically qualified for arduous duty even though the stated physical and medical requirements are not met, the field office Special Agent in Charge (SAC) or a designated representative will interview the examining physician to obtain a complete evaluation of the deficiency and a clear understanding of the medical reason for certifying the SA's ability to perform all the duties of his/her position.

(2) Specific attention will be paid to the requirement for the SA to operate a motor vehicle extensively and/or to use firearms. The results of the interview with the examining physician should be forwarded to Code 10A. The Deputy Assistant Director for Personnel Operations and Services will make the decision on retention of the employee in a SA position. Those individuals who are judged physically unqualified will be processed in accordance with 5 CFR 831 (disability retirement) or 5 CFR 339 (medical disqualification), as appropriate.

g. Physical Fitness Program. To ensure continued health, effectiveness and longevity, SAs are encouraged to maintain high standards of physical fitness. Particular emphasis is placed on those activities that improve aerobic conditioning and cardiovascular endurance.

(1) Physical fitness and employee wellness are key issues in both the public and private sectors. Employers recognize that physical fitness pays dividends in terms of reduced sick leave; reduced disability retirements, fewer accidents; increased productivity, and higher employee morale. A higher level of fitness is particularly important to law enforcement personnel, as it increases confidence and alertness; increases the capacity to withstand fatigue and stress; and, most importantly, increases the chances of survival in a deadly force encounter.

(2) A SA is considered to be in good physical condition if he/she possesses an efficient cardiovascular respiration system (good aerobic conditioning), moderate to low levels of body fat, and adequate levels of muscular strength, flexibility, and endurance. An individual who possesses these attributes is capable of performing daily assignments without undue risk of injury or fatigue and possesses sufficient energy reserve to meet unexpected physical challenges.

(3) The NCIS Physical Fitness Program contains four parts. Events include sit-ups, push-ups, bend and reach, and a 1.5-mile run. The events were selected because they do not rely on complex apparatus for preparation or administration.

(4) The Special Agent Physical Fitness Classification Table, graduated for both sex and age, enables the individual SA to assess his/her personal performance against national norms. The standards are designed to serve as a benchmark against which to judge personal performance, and are available through field office trainers.

46-6. APPOINTMENT TO A SPECIAL AGENT POSITION

a. Initial Hiring. Upon making a decision to hire an individual, the Deputy Assistant Director for Personnel Operations and Services, in consultation with the Assistant Director, Planning and Evaluation, determines the field office to which the applicant will be assigned. The applicant is notified by telephone and in writing of his/her selection, the entrance grade, initial duty station and when and where to report.

(1) If there are no openings when the processing is completed, then the applicant will be considered for future vacancies. Code 10A will advise the applicant in writing indicating his/her application will remain on file.

(2) If it is determined during or at the completion of the processing that an applicant will not receive further consideration for a SA position, Code 10A will notify the applicant of non-selection in writing. The applicant may not re-apply for one year following the date of the non-selection letter.

b. Updating Physical Information. When an applicant is hired, a limited physical examination will be required if the applicant's original examination is over six months old. This limited examination will consist of height/weight, eyesight and blood pressure verification.

c. Security Clearances.

(1) The pre-employment background investigation conducted by NCIS will meet DOD criteria for an interim security clearance, provided the investigation was completed within the past year. However, if the investigation is more than a year old when the applicant is actually hired, the NCISHQ Security Division will supply the necessary data to OPM, requesting an updated background investigation.

(2) DIRNCIS is the command authority for granting security clearances for SA personnel. The NCISHQ Security Manager upon completion of the requisite background investigation will issue the clearance certificate.

d. Initial Hiring/Entry Grade Level.

(1) The entry level for a SA with a Baccalaureate degree and limited experience is the GS-7 grade level. Hiring levels may be progressively higher depending on education and/or experience. Grade level restrictions for current Federal Civil Service employees, or, those who held a permanent Federal Civil Service position during the previous 12 months, can be found in 5 CFR Part 300 Subpart F.

(2) When the NCISHQ Special Agent Hiring Board decides that an applicant is suitable for employment as a SA, the applicant will normally be offered a position at the GS-7 Step 1 level. However, the Deputy Assistant Director for Personnel Operations and Services, may authorize the hiring of an applicant at other than the GS-7 Step 1 level if one of the following conditions apply:

(a) If the applicant is a full-time permanent federal employee in other than the 1811 series, at a grade or step above GS-7 Step 1, he/she may be offered employment at the GS-7 level commensurate with his/her current federal salary, not to exceed GS-7 step 10.

(b) If the applicant is a full-time permanent federal employee in the 1811 Series at the GS-7 through GS-13 level, he/she may be offered employment at his/her current grade and step.

(c) If the applicant is a full-time permanent NCIS employee in other than the 1811 series, at a grade or step above the GS-7 step 1 level, who possesses at least two years of NCIS experience in a position which requires thorough knowledge of criminal investigative techniques or counterintelligence/terrorism analysis, he/she may be offered employment at the GS-9 level at a step commensurate with his/her current salary, not to exceed GS-9 step 10.

(d) If the applicant satisfactorily has completed, within 12 months of the initial interview, 2 years of active duty in a U.S. military investigative, counterintelligence, or intelligence agency, he/she may be offered employment at the GS-9 level.

(e) If the applicant has a law degree from a U.S. accredited institution and has passed a state bar exam, he/she may be offered employment at the GS-9 level.

(f) If the applicant has a master's degree, or two full academic years of graduate education, in one of the following areas, he/she may be offered employment at the GS-9 level:

Accounting
Behavioral and Social Sciences
Biology
Business Management
Chemistry
Computer Information Systems
Computer Science
Criminal Justice
Criminology

Economics
Engineering
Finance
Forensic Science
Government and Politics
History
International Law
International Relations
International Studies
Justice
*Language (Arabic, Chinese, French, German, Greek, Italian, Japanese, Latin, Portuguese, Russian, Spanish, Farsi, Turkish)
Law
Middle Eastern Studies
Physics
Pre-Law
Psychology
Public Administration
Sociology
Statistics and Probability
Urban Studies

*Other languages may be considered, as necessary, based on the needs of the service.

(g) If the applicant has 2 years of significant criminal investigative experience, he/she may be offered employment at the GS-9 level. (Such experience must have required the use of recognized investigative methods and techniques.)

(h) If the applicant has 2 years experience as a uniformed law officer where at least 50% of the specified duties were directly related to criminal investigations, he/she may be offered employment at the GS-9 level.

(i) If the applicant, as a member of the U.S. Armed Forces, satisfactorily served as a credentialed SA with a military criminal investigative organization for at least 2 years, he/she may be offered employment at the GS-11 level.

(j) If the applicant has a PhD, or equivalent doctoral degree, or 3 full years of higher-level graduate education leading to such a degree, in one of the areas of study noted above, he/she may be offered employment at the GS-11 level.

(k) If the applicant, as a member of the U.S. Armed Forces, satisfactorily served as a credentialed SA with a military criminal investigative organization for at least 3 years, he/she may be offered employment at the GS-12 level.

(l) Former NCIS SAs may be rehired within 1 year at the same grade and step up to the GS-13 level. The Deputy Assistant Director for Personnel Operations and Services will decide all other rehire grades and steps on an individual basis.

(3) Eligibility for within grade (step) increases will be consistent with federal personnel regulations.

(4) All new agents must serve 1 year in grade as an 1811 before being eligible for promotion to the next higher grade in the career ladder.

e. Training/Orientation of a Newly Hired Special Agent.

(1) Typically, a new SA will be ordered to attend the Criminal Investigators Training Program (CITP) and Special Agent Basic Training Program (SABTP) shortly after coming on board. Before reporting to CITP/SABTP, the agent will be assigned directly to a Field Office where administrative tasks will be performed; e.g., completion of required documents. The new agent will not be involved in operational functions. If the CITP/SABTP course is not available within the first 30 days, the assigned Field Office will provide a program of field training/orientation until the agent attends the basic course.

(2) Responsibilities of a field office in training of newly hired agents are set forth in NCIS-1 Chapter 14. All newly hired agents who have not experienced active or reserve duty with the Navy or Marine Corps must complete the Naval Orientation Correspondence Course 16138-H. The course must be successfully completed prior to the end of the trial period. Specific information regarding this course is set forth in NCIS-1 Chapter 14.

f. Trial Period.

(1) The trial period covers the first 2 years of an SA's employment, irrespective of the grade level at which he/she was hired. If a former SA is reemployed after having been away for a year or longer, his/her 2-year trial period begins with the effective date of reappointment. If the separation from the Service has been for less than a year, prior service is creditable towards the 2-year trial period. If the SA leaves NCIS during the trial period for entry into military service, time spent on active duty or full-time reserve duty is counted toward the completion of a trial period. If the military service is not sufficient to complete the trial period, the Agent is required to complete the period upon restoration to duty with NCIS.

(2) In the event the Agent's performance during the trial period is unsatisfactory in any respect, prompt notification of his/her deficiencies must be provided to Code 10A, followed by a special Performance Appraisal Review System (PARS) evaluation. In the absence of extenuating circumstances and an affirmative recommendation to retain the SA, the Deputy Assistant Director for Personnel Operations and Services will direct the termination of the agent's employment. Acceptable performance during this trial period will be based not only on qualitative and quantitative factors related to productivity, commensurate with training and experience, but also on demonstrable indications that the employee possesses those qualities and traits requisite for career development. The long-term qualitative character of the SA corps

depends in large measure on a judicious appraisal of performance, attitude and potential during the trial period.

APPENDIX A
Special Agent Applicant
Pre-Employment Suitability Investigations

1. The agent applicant pre-employment suitability investigation (2A) is the primary resource available to the NCISHQ Hiring Board that details an applicant's lifestyle, employment record and work ethic. The following guidance is intended to ensure that the Hiring Board is provided with the most complete and accurate information available with which to make an informed hiring decision.

2. While security considerations are important and should not be minimized, they are not the primary focus of the 2A investigation. The Pre-Employment Suitability Investigation is designed to assess the applicant's ability to successfully perform the duties of a NCIS Special Agent. If the applicant is subsequently selected for employment, the Office of Personnel Management (OPM) will conduct a security background investigation.

3. Reporting should be in NCIS narrative format and incorporate the appropriate elements of

b7E

4. Specific elements to be covered during the course of the 2A investigation ("scoping") will be detailed in the NCISHQ tasking SSD. The scope of the investigation is seven (7) years from the date of the ALS (Open) or the applicant's eighteenth birthday, whichever is shorter. The required elements to be covered include but are not limited to the following:

a. **Birth** - confirm through education, employment or other available documentation.

b. **Education** - verify dates of attendance, graduation/degree, grade point average and any disciplinary actions of last college or graduate school only, if outside the scope. If within scope, verify attendance information at any business, trade, or college/university. Conduct interviews of professors/instructors, if applicant graduated within the last 3 years. Review any examples of applicant's writing.

c. **Employment** – verify dates of employment, position(s) held, review evaluations summarizing efficiency, work habits, attendance, reason for termination, eligibility for re-hire, written/oral communication skills. Review military service record and/or civilian personnel records (OPF). Conduct interview of supervisors and at least two co-workers at each of the applicant's current and former employments within the scope. Review any examples of applicant's writing.

d. **References and Developed Informants** – interview a combination of five (5) listed references or developed informants. **Interview ALL ex-spouses.**

e. **Neighborhood Inquiries** – conduct interviews of at least two (2) neighbors for each residence of six months or longer within the last 5 years. Review military housing records, if applicable.

f. **Credit Checks** - a credit check will be completed by NCISHQ Code 10A prior to the initiation of the 2A. Credit discrepancies may need to be resolved during the investigation and will be tasked in the ALS(OPEN).

g. **Local Agency Checks (LACs)** - conduct LACs for all jurisdictions where applicant has resided or been employed within the scope.

h. **Family Advocacy Program (FAP)** - FAP files should be reviewed for all military affiliated applicants including spouses.

i. **Length & Frequency of Contact** - In all interviews determine the length of time that the interviewee has known the Subject (month and year) and the frequency of contact (i.e., weekly, monthly). This should be reported in the interview IA.

j. **Contact with Subject** - It is incumbent upon the subject to provide additional or supporting information when problems are encountered locating files/witnesses, i.e., personnel files, coworkers, supervisors. All contacts with subject, whether in person or by telephone, should be documented in the ROI. If derogatory information is surfaced which may deem the candidate ineligible for employment, prior to contact with subject being initiated, coordination with Code 10A is required.

5. Should derogatory information be developed, the investigation should be expanded as necessary to fully corroborate or refute the information. Investigative leads should be forwarded as required.

6. 2A lead coverage should be completed ASAP but NLT 30 days from date of receipt.

APPENDIX (B)

281506 13:09 20111229 IN:SSDEMAIL #67501 OUT:NCISWWSSD #307

GENERAL ADMINISTRATION 29DEC11

FROM: 0000 GEN: 11C-0044

TO: DIST

SUBJ: POLICY DOCUMENT NO: 11-26: ADMINISTRATIVE (SPECIAL AGENT PERIODIC PHYSICAL EXAMINATION REQUIREMENTS)

REFERENCES

(a) NCIS 1, Chapter 13, Special Agent Career Program/Mar08
(b) NCIS 1, Chapter 46, Recruitment, Screening, and Selection of Special Agents/Dec06

1. The purpose of this policy Gen Admin is to revise reporting requirements and roles and responsibilities of the special agent (SA) and field operations support officer (FOSO) for the management of the required SA periodic physicals contained in references (a) and (b).

2. SAs have an affirmative duty to comply with the requirements of references (a) and (b). Failure to comply may result in disciplinary action. Periodic SA physical examinations are necessary for certifying that the SA is physically capable of performing arduous physical duties without hazard to the SA or others, and will be conducted within 30 days before or after the SA's birthday at ages 24, 27, 30, 33, 36, 38, 40, and annually after the age of 40.

3. The following changes to references (a) and (b) are effective immediately:

a. All previous paper forms for recording the results of SA physical examinations (to include the SF 600 Record of Medical Care) have been replaced in Navy medical facilities by an online system called PC Matrix. PC Matrix includes all of the information necessary to perform the SA physical evaluation. Navy medical providers record the results of the physical exams directly in PC Matrix.

b. A single form, "Physician's Written Opinion," (PWO) is produced by PC Matrix upon completion of the physical, and will be provided to the SA to document the results of the physical
evaluation. The form, signed by the medical provider, indicates whether the SA is physically or not physically qualified to perform SA duties and contains no other medical data. A copy of the PWO will also be mailed to Code 10D by the Navy medical facility.

c. Code 10D is responsible for updating TWMS confirming the SA's compliance with the requirements of references (a) and (b).

d. FOSOs and Headquarters office managers are no longer required to mail a copy of the periodic physical certification to NCIS headquarters.

29DEC11

SUBJ: POLICY DOCUMENT NO: 11-26: ADMINISTRATIVE (SPECIAL AGENT PERIODIC PHYSICAL EXAMINATION REQUIREMENTS)

e. FOSOs and Headquarters office managers will continue to ensure SAs complete their periodic physicals per references (a) and (b).

f. SAs are responsible for initiating and attending the examinations at the required times.

4. The changes contained in this policy will be incorporated into the next scheduled revision of NCIS 1, Chapters 13 and 46.

5. The point of contact for this document is, DAD (b)(6) Human Resources, Leadership Development Program (b)(6) @navy.mil.

DISTRIBUTION:
NCISHQ: All Directorates and Departments
INFO: WWSSD

NCIS-1 CHAPTER 47
CENTRAL FORMS MANAGEMENT
EFFECTIVE DATE: JANUARY 2014

Table of Contents

REFERENCES:
(a) SECNAV M-5213.1, Department of the Navy (DON) Forms Management Manual, December 2005
(b) SECNAVINST 5510.36A, "DON Information Security Program (ISP) Regulations", 6 October 2006
(c) SECNAV M-5210.1, (DON) Navy Records Management Program, January 2012

47-1. Purpose. This chapter establishes NCIS' policy, assigns responsibilities, and provides specific procedures for management of NCIS forms. This policy applies to all forms regardless of media, whether paper or electronic. This chapter covers the complete lifecycle management of forms from creation, distribution, use, review, and revision to cancellation.

47-2. Policy. NCIS forms management activities and policies are maintained in compliance with policies specified in reference (a). DoD's forms management policy standardizes forms throughout DoD. A form should be standardized to its highest level of use so that the common functionality of the form is shared, and the total number of different forms used within the DoD community is minimized. As the scope of forms users broadens, forms should be expanded to the appropriate level and forms designations should be changed to reflect the scope of new usage. NCIS shall follow forms hierarchy and precedence as prescribed by the Department of the Navy (DON).

47-3. Cancellation. NCIS 1, Chapter 7, Central Forms Management dated September 2007.

47-4. Background

a. Form. A tool with fixed arrangement of captioned spaces designed for entering and extracting a predetermined set of prescribed information to support DON and NCIS objectives. Additional DON forms definitions may be found in Appendix A. Only DON civilians (not including contractors) and military personnel, are authorized to serve as the point of contact, provide coordination on, certify,

and/or approve official DON and NCIS forms.

b. Forms management ensures that forms collect needed information effectively, efficiently, and economically. Collecting information is vital to the success of NCIS and provides the basis for management decisions. NCIS' centralized forms management process ensures that appropriate forms are available to collect specific data needed to meet individual requirements in a quick and efficient manner. As information requirements change, an effective NCIS-wide forms management process is critical to improving and maintaining control of authorized forms. NCIS forms management activities and policies are maintained in accordance with reference (a).

47-5. DON Forms Heirarchy and Precedence

a. It is DoD Forms Management policy to standardize forms throughout DoD. The type of form used is determined by the scope of its intended use, and is indicated by the form designation. There is an established hierarchy of authorized forms. A form should be standardized to its highest level of use so that the common functionality of the form is shared, and the total number of different forms used within the DoD community is minimized. As the scope of forms users broadens, forms should be expanded to the appropriate level and forms designations should be changed to reflect the scope of new usage. NCIS shall follow forms hierarchy and precedence as prescribed by DON.

Level	Type	Description
FIRST	Standard Form (SF) Optional Form (OF)	Established for government-wide use. The use of a SF is mandated by a prescribing directive, regulation, or law. DON personnel shall not create any form that duplicates SF or OF Forms.
SECOND	Department of Defense (DD) Forms	Established for DoD-wide use. DON personnel shall not create any form that duplicates a DD Form.
THIRD	DON-wide Forms (i.e., SECNAV, OPNAV, NAVMC)	Established for use in more than one command.
FOURTH	Internal Forms (i.e., NCIS, NAVSEA, NAVAIR, etc.)	Established for use within a specific Navy/Marine Corps command.
FIFTH	Internal Forms (i.e., NCIS Field Office, SUPSHIP, NAVAIR DEPOT, etc.)	Established for use within a specific Navy/Marine Corps field office/activity (Echelon 3 or lower).

b. Items Not Managed as Forms

(1) Office forms used only within the originating division, branch, section, or field office.

(2) One-time forms to satisfy a one-time requirement, are not re-used or reprinted, and are obsolete when the expiration date is met. One-time forms must include the statement in parentheses "one-time" following the form number, and show the expiration date next to it (for example, "One-Time, Expires 20 January 20XX").

(3) Test forms established to be used for a limited period of time so they may be evaluated before becoming permanent. Life of a test form may not exceed one year. Test forms must include the statement in parentheses "Test" following the form number and show the expiration date next to it.

(4) Forms used only once as part of a survey.

(5) Checklists used as workflow guides.

(6) Formatted documents without spaces for entering information, such as instruction sheets and bulletins, pamphlets, notices, certain tags and labels, guide letters and form letters.

47-6. Roles and Responsibilities. Reference (a) requires DON activities to maintain a centralized forms management program. The NCIS Forms management program is resident in Code 11C2, Central Administration Branch. Code 11C2 analyzes requests for new or revised forms and related procedures to effect improvements to meet forms management objectives, DON forms standards, to prevent unnecessary forms creation, and to ensure adequate instructions for using forms are provided. Within NCIS, the Code 11C2 forms manager is responsible to:

a. Serve as organizational policy subject matter expert for administration of NCIS forms.

b. Serve as NCIS Echelon II forms representative to DON.

c. Develop or improve data elements and forms design of proposed or existing forms.

d. Review, coordinate, and approve forms to ensure efficient gathering of information that is responsive to management requirements.

e. Oversee and coordinate NCIS forms management functions which include administration of reports, directives and other forms management improvement efforts, forms maintenance, printing, forms stocking, and distribution.

f. Maintain the master list of authorized NCIS internal and DON sponsored forms.

g. Maintain form history files and a list of authorized NCIS internal forms numbers.

h. Coordinate approval for NCIS sponsored DoD and DON forms.

47-7. Official NCIS Forms Repository. The Lighthouse Forms website is the official source for obtaining approved NCIS forms. Appendix B provides additional websites where approved DoD, DON, and OPM forms can be found.

47-8. Creating NCIS Forms. Program objectives may require a need to develop NCIS form(s) when higher hierarchical forms are not available, or do not capture all required data elements. Originating offices shall submit proposed form(s) for review and approval to Code 11C2 along with a draft Gen Admin (Appendix C) announcing the requirements for the use of the form and the green blazer (NCIS Form 5000.8D). Request should be sent to (b)(7)(E) @navy.mil via e-mail. Code 11C2 is responsible to ensure that the proposed forms:

a. Comply with DoD and DON privacy act, records management, and security requirements.

b. Comply with DON Forms Design guidelines and standards illustrated and described in Appendix D, Sample Navy Form.

47-9. Forms Revision and Cancellation

a. Personnel may not change or modify existing NCIS forms to suit individual needs. Changes to formatting or standard templates require review and approval by Code 11C2.

b. Any time a form requires revision for any reason, i.e., internal electronic functioning, or change in data elements, the form will be re-dated to indicate a revision was made.

c. Forms will be reviewed every two years to identify opportunities for standardization, elimination of duplicate or unnecessary forms, and to improve form effectiveness. The NCIS forms manager will complete this review with the assistance of form originator.

d. Rescinding a Form. A form becomes obsolete when another form supersedes it, when the originator rescinds it, or when the prescribing NCIS Manual/Chapter directive is rescinded. Links to obsolete forms will be removed from Lighthouse and Code 11C2 will release a Gen Admin to notify users of forms cancellation. NCIS' forms manager and form originator are responsible for ensuring that any reference made to obsolete forms are removed from active publications and web links.

47-10. Legal and Security Requirements

a. Privacy Act of 1974 (5 U.S.C. 552a). Forms that collect personal data from individuals for inclusion in a Privacy Act system of records (a collection of records retrieved by an individual's name or personal identifier), and forms that request the individual to enter or verify the social security number, normally must contain a Privacy Act Statement. However, a Privacy Act Statement is not required in the collection and maintenance of information for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual. Privacy Act Statements allow individuals completing the form to make an informed decision about whether to furnish the information. Coordinate all proposed new or revised forms that collect personal data with the Privacy Act Officer and Legal Counsel.

b. Social Security Number (SSN) Reduction. Compliance with provisions of the Privacy Act as outlined in section 47-10, paragraph (a) must also be followed whenever SSNs are used in a business process. Failure to comply with the Privacy Act may result in civil actions and or criminal penalties. Official NCIS forms containing SSN fields must be reviewed by the Privacy Act officer and justified using the SN 5213 Mar 2010 form. Acceptable uses of the SSN are those that are provided for by law, required for interoperability with organizations beyond the DoD, or are required by operational necessity. Operational necessity may be the result of the inability to alter systems, processes, or forms due to cost or unacceptable levels of risk. Ease of use or unwillingness to change are not acceptable justification for use of the SSN. Command or installation justification shall be reviewed at least one administrative level above the senior signing official. The justification section must be signed by an SES, Flag, or General Officer or personnel with by direction authority. If a justification for SSN use is rejected, the originator of the form will ensure immediate steps are taken to eliminate the SSN data field or eliminate the form.

c. Classified Forms. Classified forms must have markings required by reference (b). Classified forms must exhibit appropriate security classification markings and indicate any downgrading, declassification, or review instructions.

d. Records Management. Execution of processes and procedures prescribed in forms results in the creation of records that document the business of NCIS. Maintaining an accurate record set for each form issued by NCIS is a responsibility mandated by law, and the record set for a form must be maintained in the file history as required by reference (c).

APPENDIX A:
ADDITIONAL RELEVANT FORM DEFINITIONS

Adopted Form	A form in this category is initiated by two or more Navy components. Use is prescribed by a regulation, manual, or instruction from each of the respective components who initiate the form.
Automated Form	All forms created, stored, transmitted, filled-in, filed and destroyed electronically. There is no paper involved in this process.
Electronic Data Interchange (EDI)	A paperless computer-to-computer exchange of routine business documents.
Electronic Form	An officially prescribed electronic arrangement of captioned spaces designed for entering and extracting prescribed information. The electronic medium uses an exact sequence prescribed by the issuing component or is a mirror-like image of the officially prescribed form. There are basically two types of electronic forms; one that is part of an automated transaction, and one where the image/data elements reside on a computer. These forms can be integrated, managed, processed, and/or transmitted through a component's information processing workflow systems, with permission of the originator, via the FM. a. Automated Form. A form created, stored, transmitted, filled-in, filed and destroyed electronically. There is no paper involved in this process. b. Flat Sheet Print on Demand Form. A form created, transmitted, and stocked electronically, but printed, filled-in, filed and stored on paper. c. Computer Generated Form. A form designed for various computer systems. d. Electronic Data Interchange (EDI). A paperless computer to computer exchange of routine business documents.
Flat Sheet Print on Demand Form	A form created, transmitted, and stocked electronically, but printed, filled-in, filed and stored on paper.
Format	A guide, table, sample or exhibit that illustrates a predetermined arrangement or layout for presenting information. Most formats are largely narrative in nature and the space needed by the respondents to furnish the desired information varies substantially. Formats are often used where the arrangement and layout of items are simple and flexible and where the number of respondents is fairly limited. A format is used instead of a printed form in such instances, requiring a less expensive and more effective method of collecting desired information. Formats should not be used in place of a standardized form or to expedite a project. Formats often place an unnecessary burden on the respondent and fail to provide needed data.
Forms Index	An electronic file containing at a minimum the form number, title, edition date, requiring directive, report symbol (when applicable), originator/sponsor including contact information, and stocking/distribution related information.
Office Form	A form approved by the FM for use within only one office of a command or subordinate command. An office form does not collect data to be used outside of that office and cannot replace the collection of data required on a higher level form. It does not have to be prescribed by a directive.
One-Time Form	Developed for use for a specific project having an established termination date.
OPNAV Form	Second highest level form within the DON.
Prescribed Form	Requires mandatory use for all Navy components to whom the subject matter applies. Form is prescribed by a DON issuance.
SECNAV Form	Highest level form within the DON.

APPENDIX A (CONTINUED):
ADDITIONAL RELEVANT FORM DEFINITIONS

Specialty Form	Certain printed items that may not have fill-in spaces, such as tags, labels, and posters, may be considered as forms if they are to be stocked in the Navy supply system. These items must also be mentioned in a requiring instruction, notice, or order. If these forms are not stocked in the Navy supply system, form numbers are not required.
Stock Number	Both GSA and DON use stock numbers to identify and order forms. Information for GSA stock numbers is contained in the "Standard and Optional Forms Facsimile Handbook" published by GSA. All DON paper/specialty forms stocked and listed on Navy Forms Online (http://forms.daps.dla.mil) are assigned stock numbers by the Document Automation & Production Service (DAPS).
Unauthorized Form	An uncontrolled form, issued without an identifying prefix or number, or given a prefix or number without the approval of the FM. These forms are not compatible with any particular method of completion. Unauthorized forms need not be completed. Persons receiving unauthorized forms have the authority to reject use of the form.

APPENDIX B:
NCIS AND OTHER GOVERNMENT AGENCY FORMS WEBSITES

Office of Personnel Management

b7E

Department of Defense

b7E

Department of the Navy

b7E

NCIS

b7E

APPENDIX C:
SAMPLE GEN ADMIN

GENERAL ADMINISTRATION DDMMMYY

FROM: 0000 GEN: XX-XXXX

TO: DIST

SUBJ: UPDATE/AVAILABILITY/CANCELLATION OF NCIS FORM XXXX/XX, TITLE OF FORM

1. The purpose of this Gen Admin is to announce the update of NCIS Form XXXX/XX – TITLE OF FORMS, (Rev. 12-11) used to XXXXXXX.

2. The updated title of form (identify the purpose of the requirement/update/cancellation).

3. The updated form is available to view, print, and/or download from Lighthouse.

4. The point of contact for this document is XXXX. He/She can be reached at (b)(6) -XXXX or XXXX@navy.mil.

DISTRIBUTION:
NCISHQ: All Departments and Directorates
INFO: WWSSD

APPENDIX D:
SAMPLE NAVY FORM

CLASSIFICATION STATEMENT IF APPLICABLE - FONT ARIAL 8 UPPER CASE

REPORTS SYMBOL AND EXPIRATION DATE - FONT ARIAL 8 UPPER CASE
REQUIRING DIRECTIVE DESIGNATION - FONT ARIAL 8 UPPER CASE

1.5 point or 1/48" (0.021) solid border line for all four sides. Use 1/2" page margins..

SAMPLE FORM

TITLE - Font Arial 10 UPPER CASE

Privacy Act - Font Arial 8 Upper and Lower Case

Statements with words **AUTHORITY**, **PRINCIPLE**, **PURPOSE**, **ROUTINE USES**, and **DISCLOSURE - Font Arial 8 Bold UPPER CASE**

1. CAPTION - Font Arial 8 UPPER CASE	2. CAPTION - Font Arial 8 UPPER CASE
Fill Text - Font Times New Roman 10	Fill Text - Font Times New Roman 10
3. CAPTION - Font Arial 8 UPPER CASE Use "hairline" (0.003) lines within sections.	4. CAPTION - Font Arial 8 UPPER CASE
Fill Text - Font Times New Roman 10	Fill Text - Font Times New Roman 10

SECTION TITLE - ARIAL 8 B0LD UPPER CASE

Use 1 point or 1/72" (0.014 solid lines for dividing primary sections.

5. CAPTION - Font Arial 8 UPPER CASE	6. CAPTION - Font Arial 8 UPPER CASE
Fill Text - Font Times New Roman 10	Fill Text - Font Times New Roman 10
7. CAPTION - Font Arial 8 UPPER CASE	8. CAPTION - Font Arial 8 UPPER CASE
Fill Text - Font Times New Roman 10	Fill Text - Font Times New Roman 10

9. CAPTION - Font Arial 8 UPPER CASE

Fill Text - Font Times New Roman 10

10. CAPTION - Font Arial 8 UPPER CASE	11. DATE - Font Arial 8 UPPER CASE
Fill Text - Font Times New Roman 10	Fill Text - Font Times New Roman 10 Date Format: DD MMM YYY

Agency Disclosure Statement - Font Arial 8 Upper and Lower Case

Fill Text - Font Times New Roman 10

FORM NUMBER AND EDITION DATE - Font Arial 8 UPPER CASE

SUPERSESSION STATEMENT - Font Arial 8 UPPER CASE

APPENDIX D (CONTINUED):
SAMPLE NAVY FORM

Use the following design standards in the preparation of Navy/Marine Corps forms, except when precluded by special requirements or the functional use of the form:

a. Form Size

(1) If printed, forms should be designed to 8-1/2 x 11 inches.

(2) Postcard forms must measure a minimum of 3-1/2 x 5 inches, a maximum of 4-1/4 x 6 inches.

(3) Two-page forms are not required to be printed front and back unless required by originating/sponsoring office.

Note: There are instances when designing and/or printing forms on other than standard size paper is mandatory; for example, some OSD/Washington Headquarters Services and Navy/Marine Corps programs require forms on paper larger than standard size. In these special instances the command FM can authorize designing and printing forms on other than standard size paper.

b. Border/Margins of the Form

(1) Use a 1.5 point or 1/48" (.021) solid border for all four sides, if applicable.

(2) Unless the form has special requirements, use 1/2 inch page margins.

(3) Use 1 point or 1/72" (.014) solid lines for dividing primary sections.

(4) Use "hairline" (.003) lines within sections.

c. Layout of the Form

(1) When designing, the grid size should be 1/10 horizontal, 1/6 vertical.

(2) Forms are designed in box style with fillable fields having upper left captions.

(3) Lay-out and number items in sequential order of fill-in. Numbers shall be in the upper left corner immediately before the box caption.

(4) Group common items together on the form. Sections may be used. If several data elements pertain to the same area, individual, etc., use a section. The section title should be set flush-left margin.

(5) National Archives and Records Administration requires a separate field or block for the signature field and for the signer's printed/typed name.

(6) All mail or self-mailers must conform to current U. S. Postal Service regulations.

d. Type of Font Styles for the Form

APPENDIX D(CONTINUED):
SAMPLE NAVY FORM

(1) Text fonts are Arial 8 point, or equivalent, and all fill fonts are 10-point Times New Roman, or equivalent.

Note: For special cases, font sizes may be adjusted with FM approval.

(2) Use comparable italic (optional) for words, phrases, or instructions in parentheses.

e. Title, Number, and Data of the Form

(1) Form Title. Place the title at the top of the form, centered, inside the border (if applicable). Ensure the title is brief, specific, and meaningful. Eliminate any unnecessary words, such as form, label, etc. For commands that require a title to be placed somewhere other than the top center, approval will be required from the cognizant FM.

(2) Form Number and Date. Place the form number and edition date at the bottom, left margin, outside of the border (if applicable). For commands that require a form number to be placed somewhere other than the bottom left, approval will be required from their FM.

(a) The form designation is shown in full capital letters and indicates the scope of use for the form, i.e., SECNAV, OPNAV, NAVMC, command, or installation-wide. The form designation for forms used Navy-wide is "SECNAV", "OPNAV", or "NAVMC" for Marine Corps-wide.

(b) The form designation is followed by the form number, which is assigned sequentially as new forms are created. Previously assigned form numbers are NOT reused.

(c) The edition date consists of the month and year that the edition of the form is approved. The edition date is displayed as MM/YYYY. Example "04/2005" immediately following the form number in parenthesis.

f. Suppression Notice. Immediately follows the edition date centered at the bottom of the form. Standard suppression notices used on forms include:

"PREVIOUS EDITIONS ARE OBSOLETE"
"PREVIOUS EDITIONS WILL BE USED"
"REPLACES (Type of Form), WHICH IS OBSOLETE"

g. Requiring Directive Designation. Forms users need a way to identify directives calling for the use of a particular form, therefore, the designation number of the requiring directive is shown in the upper right-hand corner on the face page.

APPENDIX D (CONTINUED):
SAMPLE NAVY FORM

Form Part	Font Size	Letter Casing
Form Title	10 point	Upper case
Agency Disclosure Statement	8 point	Upper and lower case
Privacy Act Statement With words AUTHORITY, PRINCIPLE PURPOSE, ROUTINE USES and DISCLOSURE	8 point 8 point Bold	Upper and lower case Upper case
Section Titles	8 point Bold	Upper case
Captions	8 point	Upper case
Form Number and Edition Date	8 point	Upper case
Super session statement	8 point	Upper case
Requiring Directive Designation	8 point	Upper case
Report Symbols	8 point	Upper case

NCIS-1, CHAPTER 48
NCIS HEADQUARTERS EMERGENCY ACTION PLAN
EFFECTIVE DATE: SEPTEMBER 2013

TABLE OF CONTENTS

48-1. Purpose. To outline responsibilities and provide general guidelines for conducting operations, protecting personnel and property, and restoring essential operations to prevent loss or compromise of classified information in emergency situations at Naval Criminal Investigative Service Headquarters (NCISHQ) during natural disasters, major accidents, or hostile actions.

48-2. Policy. This Emergency Action Plan (EAP) establishes policies and outlines responsibilities and general procedures for the sheltering and emergency evacuation of NCISHQ personnel during emergency situations. It further provides general procedures for NCISHQ personnel for the safeguarding, evacuation and/or destruction of sensitive compartmented information (SCI) and other classified material during emergency situations. This plan applies to NCISHQ personnel and NCISHQ sensitive compartmented information facilities (SCIFs) located in the Russell-Knox Building (RKB) on Marine Corps Base, Quantico, Virginia. This plan will be reviewed annually and as required.

48-3. Cancellation. NAVCRIMINVSERVINST 3301.1A/Sep07 and Gen Admin 11C-0017/ 24Jul12/Subj: NCIS Headquarters Evacuation Plan.

48-4. Chapter Sponsor. The chapter sponsor for this chapter is the Security and Facilities Department, Code 11A.

48-5. Objective. This EAP outlines procedures for handling each of the listed emergency situations. In all instances, the senior person on duty must implement emergency procedures, as

appropriate to the given situation. NCISHQ personnel will be prepared to implement this plan upon notification by the senior person on duty, local law enforcement personnel, or other emergency response personnel. During an emergency, the plan can be retrieved and used as a quick reference guide by staff members in response to an emergency situation.

48-6. Definitions. For the purposes of this EAP and all associated documents, the term NCISHQ refers to all NCIS facilities located at RKB on Marine Corps Base, Quantico (MCB-Q). This facility is within the MCB-Q area of responsibility (AOR) and is included in the NCIS continuity of operations plan (COOP). RKB consists of six buildings: Building 1 - East Wing; Building 2 – Training; Building 3 – Keystone; Building 4 - Food and Fitness; Building 5 - West Wing; and Building 6 - Logistics.

48-7. Responsibilities

a. The RKB Security Operations Center (SOC) is the lead emergency coordinator for the RKB. At the conclusion of an evacuation event, a senior representative from each tenant organization will report the status of all personnel to the SOC. In turn, the SOC will report the status of all RKB personnel to the MCB-Q Fire or Military Police Departments.

b. Evacuation Warden (EW). The Deputy Assistant Director for Administrative Services Department is the NCIS EW; the NCIS Safety and Occupational Health Manager is the alternate NCIS EW. The EW will manage and implement the NCIS evacuation plan and coordinate with Headquarters directorates to identify fire wardens (FWs) for NCIS spaces located on the second and third floors of the West Wing, the concourse level, the first and second floors of the Keystone, and the Logistics Building. The number of FWs will be sufficient to provide adequate guidance and instruction during an evacuation event.

c. Fire Warden (FW). FWs are responsible to assist and ensure employees within their assigned area of responsibility (AOR) safely evacuate the building. FWs will familiarize themselves with the building layout and the various alternative escape routes from their AOR. The FWs shall be the last persons leaving their AOR and shall proceed to the primary NCIS rally point and report to the EW or alternate EW that their AOR has been evacuated. FWs shall also be aware of personnel within their AOR who may require assistance during the evacuation.

d. Assistant Directors (ADs), Deputy Assistant Directors (DADs), and supervisors.

(1) Supervisors at each level are responsible to account for their assigned employees. Each supervisor shall ensure an alpha roster for their HQ Code is kept current and available. Supervisors shall also be aware of personnel who may require assistance during the evacuation.

(2) ADs are responsible for monitoring employee accountability and reporting. ADs may assign a representative to perform this function. Directorate representatives must get to the rally point quickly to begin accounting for personnel. The HQ Directorate representative will report the status of their personnel (including any employees who cannot be located) to the EW or alternate EW at the primary NCIS rally point.

(3) All personnel shall be familiar with this chapter in order to ensure compliance with evacuation requirements. Supervisors shall ensure personnel receive training in safe evacuation procedures, location of the primary and alternate building exits, and location of their assigned rally point. Fire bills with floor plans, escape routes, alternate escape routes, and locations of exits and fire extinguishers are posted at the exit from each department and at all fire escapes and elevators. Code 11 has provided a diagram of the NCIS rally points (Appendix A) to each directorate.

e. Visitors. Building occupants are responsible for ensuring visitors to their areas follow evacuation procedures and go to the appropriate NCIS rally point. Visitors shall be included in the accountability report to the EW.

f. MCB-Q Military Police and Fire and Rescue personnel will provide emergency support to the RKB during an evacuation event.

48-8. General Information. The overriding consideration during any emergency is the safety of all personnel. This EAP complies with the Occupational Safety and Health Administration (OSHA) EAP as required by 29 CFR 1910.38. This EAP applies to all emergencies where employees need to be evacuated for personal safety. All personnel shall be trained in safe evacuation procedures. Refresher training is required whenever this EAP is changed, or when an employee responsible for specific evacuation duties has changed. If security for either SCIFs or secure rooms is severely degraded or rendered inoperative, specific security precautions must be implemented to ensure all classified materials remain properly secured against loss or compromise.

48-9. Fire

a. Procedure

(1) In the event of a fire, the person discovering the fire will broadcast the alarm to other building occupants.

(2) Pull the fire alarm box and notify the RKB SOC. All fires will be reported immediately, even if the fire is extinguished.

(3) The RKB fire alarm system will annunciate throughout the facility and automatically notify the fire department as to the location of the alarm. Additionally, each facility is equipped with a heat activated fire suppression water sprinkler system that will automatically activate.

(4) If the fire is small (e.g., a trash can fire) and time permits, personnel may use the fire extinguishers located in the area to put out the fire.

(5) During a fire emergency, ALL building occupants shall evacuate immediately. This includes personnel handling classified and sensitive material. The top priority in an emergency is the evacuation of all personnel; however, if time permits, secure classified and sensitive information by closing and locking security containers.

b. Amplifying Instructions

(1) Stairwells are the primary means for evacuation. Employees shall not use elevators during an evacuation.

(2) Supervisors will assign personnel by name or position to assist employees who need aid in safely evacuating the building and ensure they are trained in the use of the evac-chairs located in the RKB fire escapes. Contact the closest RKB security personnel (identified by a blue blazer) if assistance is required. Emergency response personnel will be notified.

(3) If an employee becomes injured and cannot evacuate the building without aid, then the FW or the nearest supervisor will contact RKB security personnel for evacuation assistance.

c. Evacuation procedures. These procedures are to be followed for each evacuation, regardless of the cause.

(1) When notified to evacuate the building by alarm or oral instruction from a supervisor or RKB security personnel, employees will depart the RKB immediately via the exit nearest to their location.

(2) When the fire alarm sounds, supervisors shall ensure that hearing and visually impaired personnel are aware of the emergency. Supervisors will also ensure that employees quickly secure classified documents and exit the building, if time permits.

(3) FWs shall take their emergency equipment and direct employees to the proper evacuation exits. FWs will also check workspaces, restrooms, and other associated spaces to ensure employees have evacuated their AOR.

(4) NCIS employees shall proceed to their designated rally point. The primary NCIS rally point is located across from the West Wing entrance in the northwest corner of the West A Parking lot. All personnel located in the West Wing and Keystone will report to this rally point. The rally point for personnel in the Logistics Building and the Food and Fitness Building is in the Front Parking area at the main building entrance. All employees must report to their designated rally point regardless of the exit used to leave the building.

(5) HQ Directorate representatives with signs displaying respective Codes will be located at the rally points in Appendix A so all employees can easily identify their gathering area. Supervisors and HQ Directorate representatives will work together to quickly account for their personnel.

(6) Once the FWs depart the building, they shall proceed to the primary NCIS rally point and report to the EW or alternate EW that their AOR has been evacuated.

(7) Once the HQ Directorate representatives have verified accountability for their employees and visitors, they will report the results to the EW or alternate EW (including any employees who cannot be located).

(8) Once the EW receives status reports from the HQ Directorate representatives and the FWs, he or she will notify the senior NCIS official on site and the SOC or Fire Department of the results.

(9) Authorization to re-enter the RKB will be announced by the SOC or the Fire Department. Employees cannot re-enter the building until this announcement is made.

d. Entrance of Emergency Personnel

(1) RKB SOC representatives will direct responding firefighting/emergency crews to the fire location. Allow firefighters, security forces, and medical personnel immediate access into all spaces, SCIFs, and secure rooms. Appropriately cleared escorts will provide access if practical, but under no circumstances will access be refused or restricted due to the lack of an escort.

(2) The requirement to safeguard classified material does not grant the authority to bar, or otherwise obstruct, fire and medical personnel, security forces, rescue workers, or other such emergency personnel requiring entry to the SCIFs, secure rooms, or office spaces during an emergency situation. Be prepared to:

(a) Assist emergency personnel.

(b) Conduct an inventory of classified and sensitive material to ensure none has been removed.

e. After Action Procedures. Once the area has been designated as safe for return by the fire department and/or security forces, SCIFs and other areas containing sensitive and classified materials should be secured:

(1) Determine if classified material has been exposed to unauthorized personnel. If so, the HQ Code security coordinator will identify the personnel involved and administer inadvertent disclosure agreements as necessary. Use the "Inadvertent Disclosure Briefing and Agreement" statement provided in Appendix B.

(2) If the individual(s) involved refuse(s) to sign the form, write the individual’s name on the form and annotate the form with “refusal to sign.” Then describe the circumstances involved on the form and then sign it. Provide the inadvertent disclosure statement to the Security Division.

(3) Coordinate with the Electronic Key Management System (EKMS) Custodian, Special Security Officer (SSO) and Security Manager, as necessary, to conduct a 100 percent inventory of all communications security, SCI, and classified materials respectively.

(4) Coordinate with the NCIS Security Manager/SSO to determine the security posture of SCIFs and/or secure rooms and take corrective action as needed.

(5) Provide a follow-up report to the EKMS Custodian, Security Manager, or SSO. The NCIS SSO will provide a report to the Navy SSO, if necessary.

48-10. Bomb Threat and Suspicious Package:

a. Procedures

(1) When a bomb threat is received by telephone, the receiver should:

(a) Note as much information about the call and caller as possible (time, location, place, voice, etc.). Use the Department of the Navy "Telephonic Threat Complaint" OPNAV 5580/8 (Rev. 11/2006) form shown in Appendix C to record information. Be calm, courteous, and do not interrupt the caller.

(b) Do NOT hang up. If time permits and the caller is talkative, ask questions, such as "Who is calling, please?" or "What is your name?"

(c) Call RKB SOC and report the situation. Answer questions asked by the SOC representative.

(d) Immediately notify the:

1. Supervisor.

2. NCIS Security Manager.

3. Multiple Threat Alert Center (MTAC) Watch Officer.

(e) Be prepared to evacuate.

1. Secure classified material, if possible.

2. Visually check the work area for suspicious objects. Do not touch the item. Note package markings and take personal belongings (coat, keys, purse, etc.).

3. If a suspicious package or unattended baggage is found, do not touch the item.

(f) The on-scene commander (OSC) will make the decision to evacuate. The OSC is usually the first arriving MCB-Q police officer. Once informed to evacuate, follow the procedures outlined in paragraph 48-9.c above.

(2) All bomb threats will be considered real until proven otherwise. Once a threat has been received, notify the senior person on duty.

b. Entrance of Emergency Personnel During a Bomb Threat

(1) RKB SOC representatives will direct responding firefighting/emergency crews to the potential bomb location. Allow firefighters, security forces, and medical personnel immediate access into all spaces, SCIFs, and secure rooms. Appropriately cleared escorts will provide access if practical, but under no circumstances will access be refused or restricted due to the lack of an escort.

(2) The requirement to safeguard classified material does not grant the authority to bar, or otherwise obstruct, fire and medical personnel, security forces, rescue workers, or other such emergency personnel requiring entry to the SCIFs, secure rooms, or office spaces during an emergency situation. Be prepared to:

(a) Assist emergency personnel.

(b) Conduct an inventory of classified and sensitive material to ensure none has been removed.

48-11. Natural Disaster

a. MCB-Q is subject to several types of natural disasters, including: earthquakes, hurricanes, tornadoes and high winds, severe thunderstorms and flooding, severe snow storms/blizzards and ice storms. NCIS will follow instructions from MCB-Q regarding all natural disasters.

b. NCIS employees may be directed to provide muster reports via the Navy Family Accountability and Assessment System (NFAAS). HQ Directorates will notify the NCIS MTAC Watch Officer or designated MTAC action officer when reports have been made and include accountability/incident information as directed above. The NCIS MTAC Watch Officer or designated MTAC action officer will make this information available to NCIS leadership upon request.

c. If the situation warrants and evacuation of the RKB, employees will follow the procedures outlined in paragraph 48-9c above.

d. Shelter in Place

(1) In the event of an emergency which does not require evacuation, NCIS policy may be to shelter in place. Simply stated, this means that the safest place to be in the event of certain disaster is the individual's official work duty site. Personnel should maintain a 72-hour supply of medication in the event a disaster prohibits departure or egress from RKB MCB-Q.

(2) If the decision is made by MCB-Q or NCIS senior leadership to shelter in place, all NCIS personnel should stay in their workspace unless directed otherwise. The senior person in charge will provide accountability and incident reports to the NCIS MTAC Watch Officer or other designated reporting agency.

e. Entrance of Emergency Personnel

(1) RKB SOC representatives will direct responding firefighting/emergency crews to the incident/damage location. Allow firefighters, security forces, and medical personnel immediate access into all spaces, SCIFs, and secure rooms. Appropriately cleared escorts will provide access if practical, but under no circumstances will access be refused or restricted due to the lack of an escort.

(2) The requirement to safeguard classified material does not grant the authority to bar, or otherwise obstruct, fire and medical personnel, security forces, rescue workers, or other such emergency personnel requiring entry to the SCIFs, secure rooms, or office spaces during an emergency situation. Be prepared to:

(a) Assist emergency personnel.

(b) Conduct an inventory of classified and sensitive material to ensure none has been removed.

48-12. Riot, Civil Disorder, Sabotage, Hostile/Terrorist Attacks. It is difficult to determine when the MCB-Q and/or RKB area might encounter major incidents resulting from riots, civil disorders, sabotage, or hostile/terrorist attacks. Such incidents may or may not occur without some warning. If such an incident does occur, notify the senior person on duty and implement the following procedures.

a. NCIS will follow instructions from MCB-Q regarding all emergencies. It is critical for NCIS MTAC to be in constant communications with RKB SOC.

b. Procedures

(1) Once an incident occurs, call RKB SOC at (b)(6) and report the situation. Follow the instructions of the security personnel.

(2) Notify the NCIS Security Manager at (b)(6)

(3) Depending on the situation and the assessment of the senior person on duty, the initial OSC will determine if evacuation of all staff personnel is prudent and can safely be accomplished. If an evacuation is ordered, employees will follow the procedures outlined in paragraph 48.9c above.

(4) Upon conclusion of an incident, provide a follow-up report to the EKMS Custodian, Security Manager, or SSO. The NCIS SSO will provide a report to the Navy SSO, if necessary.

(5) NCIS employees may be directed to provide muster reports via the NFAAS. HQ Directorates will notify the NCIS MTAC Watch Officer or designated MTAC action officer when reports have been made and include accountability/incident information as directed above.

The NCIS MTAC Watch Officer or designated MTAC action officer will make this information available to NCIS leadership upon request.

c. Shelter in Place

(1) In the event of an emergency which does not require evacuation, NCIS policy may be to shelter in place. Simply stated, this means that the safest place to be in the event of certain disaster is the individual's official work duty site. Personnel should maintain a 72-hour supply of medication in the event a disaster prohibits departure or egress from RKB MCB-Q.

(2) If the decision is made by MCB-Q or NCIS senior leadership to shelter in place, all NCIS personnel should stay in their workspace unless directed otherwise. The senior person in charge will provide accountability and incident reports to the NCIS MTAC Watch Officer or other designated reporting agency.

d. Entrance of Emergency Personnel

(1) RKB SOC representatives will direct responding firefighting/emergency crews to the incident location. Allow firefighters, security forces, and medical personnel immediate access into all spaces, SCIFs, and secure rooms. Appropriately cleared escorts will provide access if practical, but under no circumstances will access be refused or restricted due to the lack of an escort.

(2) The requirement to safeguard classified material does not grant the authority to bar, or otherwise obstruct, fire and medical personnel, security forces, rescue workers, or other such emergency personnel requiring entry to the SCIFs, secure rooms, or office spaces during an emergency situation. Be prepared to:

(a) Assist emergency personnel.

(b) Conduct an inventory of classified and sensitive material to ensure none has been removed.

(3) Coordinate with the EKMS Custodian, SSO, and Security Manager, as necessary, to conduct a 100 percent inventory of all communications security, SCI, and classified materials respectively.

(4) Coordinate with the NCIS Security Manager/SSO to determine the security posture of SCIFs and/or secure rooms and take corrective action as needed.

(b)(7)(E)

Pages 1126 through 1133 redacted for the following reasons:
- -
(b)(5)
(b)(7)(E)

NCIS-1, CHAPTER 49
NCIS POLICY ISSUANCE SYSTEM
EFFECTIVE DATE: JANUARY 2014

TABLE OF CONTENTS **PAGE**

References:

(a) NCIS Manual 1, Chapter 3, Executive Decision Making Process, May 2013
(b) SECNAV Manual 5210.1, CH-1, Records Management Manual, 3 July 2012
(c) SECNAVINST 5430.107, Mission and Functions of NCIS, 28 December 2005
(d) NCIS Manual 1, Chapter 2, NCIS Mission and Organizational Structure, September 2013
(e) NCIS Manual 1, Chapter 25 Standard System Document (SSD), January 2010
(f) SECNAV M-5510.36, Information Security Program, 30 June 2006
(g) OPNAVINST 5215.17, Navy Directive Issuance System, 18 June 2005
(h) SECNAV M-5216.5, Department of the Navy Correspondence Manual, March 2010
(i) United States Government Printing Office, Style Manual, 16 September 2008
(j) DoDM 5200.01-V4, DoD Information Security Program: Controlled Unclassified Information (CUI) 24 September 2012

49-1. Purpose. This chapter establishes the policy for responsibilities, requirements, and standards for the administration and maintenance of NCIS policy. Information contained in this chapter is based on the higher authorities and requirements contained in the references. The policy management program is to provide employees with timely and well-written policies that are the framework for conducting and completing organizational mission and functions. The provisions of this chapter apply to civilian employees, active duty, reserve military personnel, and contractors.

49-2. Policy. NCIS policy provides all employees with a number of references regarding NCIS organizational functions, delegation of authorities, policies, and procedures which are central to the orderly management of NCIS activities. NCIS policy is contained in NCIS manuals and Policy General Administrative (Policy Gen Admin) documents. Inherent with maintaining an effective foundation of policy is the establishment of an effective program for the management of policy contained in its various forms. The processes and procedures described in this chapter establish this management program and must be followed to create or update NCIS policy documents.

49-3. Cancellation. NCIS-1, Chapter 49, dated May 2011.

49-4. Chapter Sponsor. The chapter sponsor for this chapter is the Administrative Services Department, Code 11C.

49-5. Responsibilities

a. Director. The Director retains the responsibility to approve NCIS policy in all forms.

b. Deputy Director. The Director has delegated to the Deputy Director the authority to implement policy and guidelines. The Director has also delegated to the Deputy Director the authority to approve existing policy that has been validated as current and compliant with all applicable statutes and regulations during the required triennial maintenance review process.

c. Chief of Staff (Code 01C). Reviews all policies submitted for approval by the Director or as delegated to the Deputy Director.

d. Executive Assistant Directors (EADs), Chiefs, and Assistant Directors (ADs)

(1) Provide leadership and management oversight to ensure departments comply with the requirements of this chapter. Maintain oversight of NCIS policy within their respective areas of responsibility, ensuring the policy remains current, relevant, and in compliance with applicable statutes and regulations.

(2) Review and approve policy decision packages prior to presentation to the Director or Deputy Director for final approval, per reference (a).

e. Deputy Assistant Directors (DADs)

(1) Perform the role of policy sponsor for assigned NCIS manuals and chapters. Provide leadership and management oversight to ensure compliance with the standards and procedures contained in this chapter.

(2) Assign an action officer (AO) as the responsible individual to manage each NCIS chapter sponsored by the department. The AO is the primary individual responsible for managing the crafting, updating, and maintenance of the chapter.

f. NCIS Inspector General (Code 00I). Review NCIS chapters and Policy Gen Admins for compliance with Management Internal Control requirements and to offer expertise based on findings, recommendations, and best business practices resulting from inspection reviews.

g. NCIS Counsel (Code 00L). Review NCIS chapters and Policy Gen Admins for compliance with regulatory and statutory authorities and to offer expertise based on legal findings and rulings.

h. Deputy Assistant Director for Administrative Services (Code 11C). Exercise overall management of NCIS policy, ensuring organizational compliance with the standards and procedures contained in this chapter.

i. Branch Head, Central Administrative Services Branch (Code 11C2). Perform process management activities to include:

(1) Developing and managing policy standards and procedures.

(2) Planning, organizing, controlling, and monitoring the NCIS policy maintenance process.

(3) Maintaining the master record copy of approved NCIS manuals, chapters, and Policy Gen Admin documents.

(4) Maintaining an archive of all permanent records associated with superseded NCIS policy in all its forms in an approved DON electronic records management program, per the requirements of reference (b).

49-6. General Information

a. Policy. Policy is defined as organizational tenets and directives that guide how NCIS executes its mission, functions, roles, and responsibilities as defined in reference (c) and reference (d). NCIS policy is contained in NCIS manuals and current Policy Gen Admins.

b. Policy Management. Policy management is the effective and efficient development and maintenance of NCIS policy contained within NCIS manuals and Policy Gen Admins. This includes establishing chapter formats, editorial requirements, standards, distribution networks, maintenance cycles, and disposition.

c. Types of NCIS Policy Documents. There are two types of NCIS policy documents: (1) chapters contained within NCIS manuals and (2) temporary Policy Gen Admin documents.

(1) NCIS Manuals. NCIS manuals are the foundation of NCIS policy and contain the majority of policies, practices, and procedures that focus on organizational functions, mission, history, delegations of authority, and standards for the administration of safety, security, facilities, logistics, acquisitions, human resources, legal requirements, criminal investigations, counterintelligence, and counterterrorism operations of the NCIS.

(a) NCIS Chapter. NCIS chapters are contained within one of the approved NCIS manuals. A chapter contains policy written by subject matter experts.

(b) NCIS Handbook. NCIS handbooks provide amplifying procedures designed to ensure compliance with NCIS policy requirements. Handbooks can be included within a chapter, or appended to it, to explain extensive practices and convey effective and acceptable procedures.

(2) Policy Gen Admin. Policy Gen Admins are the preferred method for transmitting immediate policy changes throughout the organization. Per the guidance provided in reference (e), SSD transmitted Policy Gen Admins are temporary in nature and are designed to be cancelled once incorporated into the applicable chapter during the policy maintenance cycle.

d. Availability. The current version of NCIS policy is accessible electronically via the Lighthouse on the applicable unclassified or classified portals. Code 11C2 will coordinate with Code 15 as necessary to ensure policy remains accessible to the entire organization.

e. Permanent Record. Records that have been appraised as having enduring value—historical, research, legal, scientific, cultural, or other values. Permanent records are those that will protect NCIS' and Department of the Navy (DON) interests and that document primary missions, functions, responsibilities, significant experiences, and accomplishments. All NCIS policy documents are considered permanent records of the organization. As such, these documents need to be archived in accordance with the requirements published in reference (b). Permanent records include any document that:

(1) Regulates or is essential to effective administration.

(2) Establishes, revises, or supersedes manuals/chapters and Policy Gen Admins.

(3) Initiates or governs a course of action or conduct.

(4) Establishes a procedure, technique, standard, guide, or method of performing a duty, function, or operation.

(5) Establishes a form or a reporting requirement.

49-7. Policy Standards. The policy sponsor is the head of the department that has the responsibility for establishing and maintaining the NCIS manual and/or specific subject matter chapter. Typically, the policy sponsor has oversight for the program, activity, or procedures contained in the policy being sponsored. Policy sponsors shall establish internal procedures to continually monitor the currency and relevance of the chapters that they manage in order to keep policy current and ensure NCIS policy remains in compliance with current statues and regulations.

a. NCIS Manuals. The more enduring NCIS policy is contained in NCIS manuals. However, updates to these documents typically require more time, effort, and staffing to gain approval. Accordingly, a more deliberate approach to their maintenance is required.

(1) Policy Maintenance Cycle. In order to ensure policy remains current, all NCIS policy contained in manuals will be reviewed, and updated as necessary, at a minimum of every three years. All policy reviews and any required updates must be approved by the Director the month identified in the published policy maintenance schedule. Code 11C2 is responsible for publishing and updating the triennial policy maintenance schedule. The schedule will list each chapter, the associated sponsor for each, the date that the chapter was last approved or reviewed, and the month and year in which the next review/update is due.

(a) In an effort to minimize the impact on departments sponsoring numerous chapters Code 11C2 will coordinate with policy sponsors to stagger policy reviews, rather than have too many due in a short period of time. This also staggers the staffing effort required by other departments that must review the policy.

(b) Policy sponsors are encouraged to update policy earlier than the triennial maintenance cycle if sufficient changes warrant an earlier publication of the updated policy.

(2) Policy Review Requirements. It is incumbent on the policy sponsor to plan sufficient time to conduct the review and submit an updated chapter, if that is warranted. Accordingly, departments should establish internal procedures to monitor required changes to their sponsored policy throughout the three year cycle.

(a) When conducting a policy review, the sponsor may determine that the information contained in a chapter remains current and compliant with all applicable statutes and regulations. In these cases, should the Deputy Director concur, then no update is required, and a new date of approval will be placed on the chapter. The triennial maintenance schedule will reflect the next review required three years from this new date, and the re-dated chapter will be inserted in place of the chapter residing on the Lighthouse.

(b) When conducting a policy review, the sponsor may determine that the chapter requires revision. In these cases, the new version of the chapter is staffed and routed for approval. As a reminder, the policy sponsor is required to update the chapter if any Policy Gen Admins were published as changes to the chapter. Once approved, the updated chapter will be inserted in place of the chapter residing on the Lighthouse. Once the updated chapter is approved, all Policy Gen Admins associated with it will be cancelled by Code 11C2. The triennial maintenance schedule will also reflect the new approval date.

(3) Policy Case Files. Although Code 11C2 maintains the master copy of all NCIS policy, policy sponsors are encouraged to maintain a working file on each chapter sponsored. Maintaining such a file helps to ensure continuity and should facilitate a smooth transition of information as action officers change within a department. The file should contain:

(a) A copy of the current policy.

(b) A working copy of the policy with any notes taken between reviews.

(c) Copies of all Policy Gen Admins that were released related to the chapter.

(d) A copy of any executive decision packages related to a particular policy, for background and reference.

b. Policy Gen Admin

(1) The preferred method for publishing initial changes to policy is via Policy Gen Admin. These provide for the most efficient transmission of new policy and procedures to the widest audience in the shortest possible time. These documents are also available to employees via K-Net searches.

(2) Policy Gen Admins have limitations. They are not conducive to promulgating policy changes that require voluminous information, such as would be more appropriate for a complete, or

near-complete, chapter rewrite. They are also the most difficult for employees to maintain awareness of if not immediately linked to the applicable chapter.

(3) Policy Gen Admins are also temporary policy documents that should be incorporated into applicable chapters at the first opportunity. These documents will be embedded within their applicable chapter in two ways:

(a) Once a Policy Gen Admin is approved and released, Code l1C2 will immediately incorporate the document into a new version of the associated chapter by inserting the title in the front page of the chapter and attaching the Policy Gen Admin to the impacted chapter.

(b) The review conducted by the policy sponsor during the triennial maintenance cycle should identify any Policy Gen Admins issued for a particular chapter. If a Policy Gen Admin exists, the information contained in these documents must be incorporated into the chapter revision if not superseded by subsequent policy changes.

c. New Policy. As statutes, regulations, and internal processes change or emerge, new NCIS policy may be necessary. In those cases, a policy sponsor must first be identified to produce the draft documents for staffing. Once that is accomplished the sponsor should contact Code 11C2 to obtain a new chapter number.

49-8. Policy Staffing Requirements and Timelines. Whether the policy sponsor is presenting a Policy Gen Admin, a new chapter for approval, an updated chapter, or a review requiring no update; the staff action required is the same as that associated with any other executive decision package, as depicted in reference (a). Follow the procedures outlined below when submitting policy for approval.

a. Submit all policy documents for required executive decision making reviews either uploaded in the Tasker System 5 or via the Code 11C2 Customers Service group e-mail address (b)(7)(E) @navy.mil). For each policy type follow the guidelines provided below:

(1) Policy Gen Admin. Once the new Policy Gen Admin is ready for review, ensure the following are submitted: the new Policy Gen Admin; completed Green Blazer indicating AD/EAD approval; and the electronic "Word" file of all documents.

(2) New Chapter. Contact Code 11C2 to obtain a chapter number. Once the new chapter is ready for review, ensure the following is submitted: the new chapter; draft announcement Gen Admin outlining the significant chapter information; completed Green Blazer indicating AD/EAD approval; and electronic "Word" file of all documents.

(3) Chapter Update Resulting from Maintenance Review. Contact Code 11C2 to request the master copy of the chapter for edit. Once the updated chapter is ready for review, ensure the following are submitted: the updated chapter (ensuring that all published Policy Documents or Gen Admins released by your code providing revised procedural guidance are incorporated); draft announcement Gen Admin outlining the significant chapter updates; completed Green Blazer indicating AD/EAD approval; and electronic "Word" file of all documents.

(4) Chapter Review Without Update. Submit a completed Green Blazer indicating AD/EAD approval to the Deputy Director documenting completion of the required chapter review and confirming the chapter remains current as published.

b. Policy Staffing Timeline. Policy Gen Admins, new chapters, and chapter maintenance updates must be reviewed by the appropriate AD/EAD or Chief. Code 11C2 will assign a due date to complete the executive staff review. All require review by NCIS Codes 00I, 00L, 01C, and approval by the Deputy Director as delegated.

49-9. Standards for Chapter Format. Use 12-point, Times New Roman, regular for the all text in the body of the chapter. Appendix (A) is the standard chapter format template. Appendix (B) provides commonly used acronyms and frequently made mistakes.

a. Opening Basics. All chapters will identify the manual number, the chapter number, the title, and the effective date.

b. The Table of Contents. Identify key sections in the chapter and their respective page number.

c. Current Policy Gen Admin. Identify an embed Policy Gen Admin published prior to the next policy maintenance review. (If applicable).

d. Reference(s). Identify references that bear directly on the subject at hand. Ensure all references listed are current. List references alphabetically and in the order they appear in the text and always mention cited references in the body of the chapter. (If applicable).

e. Appendix(ices). Contain material which supports but is not readily incorporated into the body of a chapter. List appendices alphabetically, identify them sequentially in the body, and attach them to the end of the chapter body in the same order as they appear in the text. (If applicable).

f. The Chapter Body

(1) Required Paragraphs. All chapters must begin with four main paragraphs described below:

(a) Purpose. This paragraph is required to briefly summarize the information covered in the chapter. The purpose statement should inform readers why the chapter was issued and what information they will find. This paragraph may include references to legal, regulatory, or other factors that led to the development of chapter.

(b) Policy. This paragraph is required to briefly state what the policy is intended to accomplish. The policy statement should briefly describe the general intent with respect to the specific topic of the policy.

(c) Cancellation. List the previously published chapter which will be cancelled by the publishing of the new chapter. If nothing is cancelled then state, “None”.

(d) Policy Sponsor. This paragraph is required to identify the policy sponsor by organizational title and code.

(2) Other Subparagraphs. Identify all subparagraphs with a number or letter. Ensure to capitalize the first letter each major word of the heading and underline paragraph headings. Periods are only used if text follows the paragraph heading. Standalone headings are not followed by a period.

Use the Header/Footer Tool to insert the classification in Bold, Capitalized, Times New Roman, 13 pitch

Appendix A: Chapter Template

%

Bold, Capitalized, Times New Roman 12 pitch

Indicates hard return

NCIS- X, CHAPTER XX
TITLE
EFFECTIVE DATE: MONTH YYYY

%

TABLE OF CONTENTS **PAGE**

%

Current Policy Gen Admin:

(a) 11C-0024-2008, Gen Admin Template, Effective Date 20 Apr 08

If applicable

%

Reference:

(a) OPNAVINST 5215.17, Navy Directives Issuance System, 13 March 2005 (Reference number, reference title, and date of reference, title case)

If applicable

%

XX-1. Purpose.

Required Paragraph

%

XX-2. Policy.

Required Paragraph

%

XX-3. Cancellation. If nothing is cancelled then state, "None."

Required Paragraph

%

XX-4. Chapter Sponsor.

Required Paragraph

%

XX-5. Additional Information Regarding Paragraph Arrangements

Title will not have a period if not followed by text.

%

******a.**Arrange paragraphs following the formats below. If subparagraphs are needed, use at least two; e.g., a (1) must have a (2) and an (a) must have a (b).

Indicates number of required spaces

%

******b.**Indent each new subdivision to align under subparagraph above.

%

*********(1)*Document subdivision.

%

*********(2)*Text.

%

**********(a)*Text.

%

**********(b)*Text.

%

**********1.**Text.

%

**********2.**Text.

%

**********a.**Do not use subparagraph past this level until you have exhausted all re-paragraphing alternatives.

%

Page number is placed in the footer, one line above classification. First page is not numbered

**********b.**Text.
%
**********(1)*Text.
%
**********(2)*Text.
%
******c.**Sample Appendix Continuation follows on the next page.

Appendix A (Continued)
Chapter Template

%

1. Titling of References. When first identifying a reference ensure to list the reference number, the title, and the date in title case. When cited in the body of the chapter, designate references by the term “reference” followed by a lower case alphabetic character in parenthesis with “reference (a)” for the first reference, “reference (b)” for the second, and so on. References must be current and listed in the order they appear in the text. An example is provided above.

%

2. Titling of Appendices. When first identifying an appendix ensure to list the appendix letter and the title. When cited in the body of the chapter, designate appendices by the term “Appendix” followed by an upper case alphabetic character in parenthesis with “Appendix (A)” for the first appendix, “Appendix (B)” for the second, and so on. Appendices must be listed in the order they appear in the text. Appendices are listed in the table of contents and their page number follows in sequence with the text of the chapter. An example is provided above.

%

3. Other Important Information

%

a. Formatting. The only authorized font for NCIS directives is Times New Roman, 12 pitch. In a chapter, 2 spaces ALWAYS follow a period “.” and a colon “:” and 1 space ALWAYS follows end parenthesis “)” and a semi-colon “;”.

%

b. Classification

%

(1) Most of the NCIS chapters are unclassified. The classification of “UNCLASSIFIED” will be placed in the header and footer of all pages in bold capitalized text using Times New Roman, 13 font.

%

(2) Per the guidance provided in reference (j) unclassified documents containing "Law Enforcement Sensitive (LES)" information shall be accompany the phrase "FOR OFFICIAL USE ONLY Law Enforcement Sensitive" in the header and footer of that page. Each paragraph which contains the LES information shall be marked "(FOUO-LES)".

%

(3) The select few classified chapters are located on the NCIS Homepage on SIPRNet. Additional guidance for the marking of classified chapters is found in reference (f).

%

c. Page numbering. Do not number the first page, start on the second and consecutives pages. Center page numbers one line above the classification markings on the bottom of the page, starting with the number 2. No punctuation accompanies a page number. Ensure the font is Times New Roman, 12 pitch. Appendices are numbered in consecutive order following the last page of text for the chapter.

APPENDIX B: COMMON ACRONYMS AND COMMON MISTAKES

1. Common Acronyms. Write terms out the first time they appear in text and place the abbreviation or acronym in parenthesis following it. Use the acronym consistently thereafter: do not repeat the term.

a. "OSD" - Office of the Secretary of Defense; "DoD" – Department of Defense; or "U.S."- United States. Use acronym only; they do not need to be spelled out ever. "DoD", "OSD", or "U.S.".

b. United States Central Command – USCENTCOM; United States Joint Forces Command – USJFCOM; United States African Command – USAFRICOM.

2. Common Mistakes:

a. Use short, simple words. Limit sentences to one thought and keep them brief.

b. Avoid long, rambling paragraphs. Organize the material. When possible use paragraph heading to highlight important concepts.

c. Use "must" to denote a mandatory action; Use "will" to denote a required action in the future; Use "must" or "will" – do not use "shall".

d. Use "may" or "can" to denote an optional action.

e. Use "Military Services" vice "Armed Services".

f. Special Agent should be special agent unless specially talking about an individual. "Special Agent" Jones is the "special agent" we spoke with.

g. Always spell out the state, do not use the two letter abbreviation in the body of the chapter. "Virginia" vice "VA".

h. "Government" agency; "Federal" law; "Government" and "Federal" are capitalized when referring to the U.S. Government or Federal.

i. "e-mail" or "email"; both are valid just use them consistently throughout document.

j. "e.g." – for example (describing one of many examples).

k. "i.e." – that is (only the item mentioned apply).

NCIS-1, CHAPTER 50
CASUALTY ASSISTANCE PROGRAM
EFFECTIVE DATE: June 14, 2011

Table of Contents

References
(a) NCIS-3, Chapter 41: Response Protocol for Major Incidents Involving Naval Criminal Investigative Service Personnel
(b) DoD Instruction 1300.18 Personnel Casualty Matters, Policies, and Procedures
(c) NCIS-1, Chapter 4: Worker's Compensation

50-1. Purpose

The NCIS Casualty Assistance Program (CAP) is intended to assist civilian employees and their families in the event of an on-duty death, excused absence--whereabouts unknown (EAWUN) (equivalent to missing in action), or serious injury incident. The CAP program draws upon existing resources in the NCIS Human Resources, Communications, Legal, and Behavioral Sciences Directorates, external resources within the Department of Defense (DoD) and the law enforcement community, and establishes additional support resources such as the Family Liaison Officer (FLO) Program. Military personnel casualty or injury situations will be handled through Navy or Marine Corps channels.

50-2. Policy

50-2.1. Policy. It is NCIS policy that an appropriate NCIS employee from the field office or headquarters directorate will contact the next of kin, as designated by the Record of Emergency Data (DD Form 93), Appendix A, upon learning of the on-duty death or serious injury of a NCIS civilian employee from that field office or headquarters directorate, and provide support services as indicated in this chapter.

In cases where the next of kin are located outside the local area of the field office or headquarters, the Special Agent in Charge or the Deputy Assistant Director will contact the closest office to arrange contact with the next of kin. In the case of a deployed death or serious injury of an NCIS employee, the NCIS notification will likely be the first notification to the next of kin.

50.2.2. Reference (a) sets forth NCIS procedures pertaining to the criminal and administrative investigation of major incidents involving NCIS personnel. Those procedures shall be used whenever a major incident involving NCIS personnel occurs either as an "incident employee" or as a "victim" of a fatal or serious injury, when an NCIS employee is missing as a result of a kidnapping, or when the death or serious injury of an individual occurs in NCIS custody. An "incident employee" is defined as an NCIS employee who is involved in a line-of-duty shooting incident and/or whose actions result in serious injury.

50.2.3 Appendix B will be the notification protocol utilized whenever any NCIS employee becomes reliably informed about an on-duty death, EAWUN, or serious injury to another NCIS employee.

50.2.4. All press or public inquiries regarding an NCIS casualty incident shall be referred to the NCIS Communications Directorate (Code 00C) for response.

50.3. Cancellation. None

50-4. Chapter Sponsor. The chapter sponsor this chapter is the Human Resources Directorate (Code 10), and the Human Resources Operations and Services (Code 10A).

50-5. CAP Manager

The CAP is the primary responsibility of the CAP Manager, who reports to the Assistant Director for Human Resources, Code 10. The CAP Manager's major duties and responsibilities include, but are not limited to:

a. Administering and managing a comprehensive worldwide NCIS CAP.

b. Assisting with the development of all phases of planning, directing, coordinating, and controlling medical administration and casualty assistance operations.

c. Reviewing, developing, coordinating and recommending changes to NCIS manuals and directives as they relate to reporting, notification, search, recovery, identification of remains, entitlements, preparation, transportation of remains, selection and assignment of escorts, funeral directors services, monetary allowances, and survivor benefits.

50-6. Casualty Working Group

The Casualty Working Group (CWG) is established as the primary decision-making body for implementation and execution of the CAP. Membership is comprised of the Principal Executive Assistant Director for Management and Administration (Code 01A), Assistant Director for Human Resources (Code 10), Assistant Director for Communications (Code 00C), personnel from Human Resources Pay and Entitlements Branch (Code 10A12), personnel from the Human Resources Services Division (Code 10A2), the General Counsel (00L), and the Behavioral Science Directorate (Code 02D).

50-7. Transportation Command Regulating Command and Control Evacuation System

NCIS will use the Transportation Command Regulating Command and Control Evacuation System (TRACES), TRANSCOM's web-based system designed to coordinate and monitor patient movement between military medical treatment facilities during peacetime, contingencies and war, to track applicable NCIS patient movements. While medical personnel make decisions related to when and how to evacuate injured or ill personnel, TRACES provides rapid and accurate entry, access and reporting of this medical evacuation information from anywhere in the world. The MTAC/Law Enforcement Desk (Code 25) will be responsible for assisting the Contingency Response Field Office (CRFO), field offices, or headquarters directorates with tracking patients or remains.

50-8. Associated Organizations

The NCIS CAP Manager will maintain contact and maintain an informal networking relationship with groups sharing a similar mission of supporting fallen, missing or wounded law enforcement officers, support personnel and their families. An example of such an organization is Concerns of Police Survivors, Inc. (COPS). Navy and Marine Corps casualty assistance offices may also be of assistance in assisting the FLO in the execution of his/her duties.

50-9. Employee Assistance Program (EAP)

The EAP provides resources for all NCIS civilian employees and their families for a wide variety of problems addressing prevention and intervention and is a potential resource for personnel affected by a casualty or serious illness. EAP is available 24 hours a day, seven days a week via website (www.foh4you.com) or CONUS toll free 800-222-0364 or for overseas offices, by calling 314-387-4701 and asking the operator to reverse the charges.

50-10. Family Liaison Officer

The FLO is the cornerstone of the CAP. At least two FLOs will be appointed by each field office and headquarters directorate. The appointed FLOs will attend the Code 10B course of instruction. The FLO is the single point of contact to provide assistance to next of kin and are trained to help find answers to their concerns and questions regarding survivor's benefits and related matters. The primary duty of the FLO is to support the next of kin for a period of 60 days after the casualty or serious injury event occurs. After the 60-day period, the FLO and CAP Manager will make an assessment to determine if the FLO duties should continue or transition to long term assistance by Code 10A or the CAP Manager.

50-11. Joint Personal Effects Depot (JPED)

The CAP Manager will establish and maintain a memorandum of understanding (MOU) with the DoD JPED for support to deployed NCIS personnel. The JPED receives, safeguards, inventories, stores, processes, and determines final disposition of personal effects for all deceased, injured or missing DoD personnel.

50-12. Record of Emergency Data

a. Reference (b) mandates that the DD Form 93, Appendix A, be completed by all DoD civilian personnel and re-validated yearly. NCIS is responsible to maintain DD Form 93 for all civilian personnel. The information contained in DD Form 93 will be used to contact and assist next of kin in the event of an NCIS employee on duty casualty, EAWUN, or serious injury.

b. Additionally, all NCIS civilian employees shall enter the same data into the emergency notification section of the Total Workforce Management Services (TWMS) (military personnel are bound by different requirements and this requirement does not apply to contract personnel).

c. Hard copies of DD Form 93 shall be maintained in each field office and headquarters directorate in an area suitable for privacy sensitive data, but accessible to management on a 24/7 basis.

d. An optional NCIS form, Line of Duty death/Serious Injury Notification - NCIS 12295/1 (July 2010), Appendix C, may also be completed. Information in NCIS Form 12295/1 provides more personalized information to assist the FLO when notification of the next of kin is required. NCIS Form12295/1 shall be maintained in each field office and headquarters directorate in an area suitable for privacy sensitive data, but accessible to management on a 24/7 basis.

50-13. Worker's Compensation Program

Code 10A2 is the point of contact for the Worker's Compensation Program (WCP) as defined in reference (c). Reference (c) provides the authority and policy for providing compensation and benefits to NCIS employees who sustain a traumatic injury, or occupational illness while in the performance of duty.

50-14. DoD Worldwide Casualty System

The DoD Worldwide Casualty System (WCS) mandates organizations to prepare names and aggregated casualty statistics for use by DoD, Congress, and other federal agencies. Reference (b) states that, "Casualty reports will be submitted without delay to the appropriate Military Service Headquarters Casualty Office within 24 hours of a component learning of the casualty. Immediately report the information by telephone to the appropriate Military Service Casualty Headquarters and then submit the casualty report." The CAP Manager and Code 10A will adopt the use of the Defense Casualty Information Processing System (DCIPS) to fulfill this requirement.

50-15. Responsibilities

50-15.1. The Assistant Director Human Resources (Code 10) shall maintain overall responsibility for the CAP and policies in this chapter, ensure CWG members are apprised of their roles in the CAP and that they are able to implement the CWG when needed.

50-15.2. Code 10A shall:

a. Maintain operational control of the EAP under Code 10A2.

b. Provide a comprehensive survivor benefits information package for all NCIS personnel.

c. Adopt the use of DCIPS as detailed in section 50-12 of this chapter for the purposes of casualty reporting.

d. Post the survivor benefits information package on the NCIS web site and update information during January of each year.

50-15.3. Code 10B shall establish a training process for the FLO program. The CAP Manager will work with 10B to ensure FLOs are identified and trained in each headquarters directorate and field office.

50-15.4. CAP Manager shall:

a. Administer and manage a comprehensive worldwide NCIS CAP.

b. Develop all phases of planning, directing, coordinating, and controlling medical administration and casualty assistance operations.

c. Adopt the use of DCIPS as detailed in section 50-12 of this chapter.

d. Review, develop, coordinate and recommend changes to NCIS manuals and directives as they relate to reporting, notification, search, recovery, identification of remains, entitlements, preparation, transportation of remains, selection and assignment of escorts, funeral directors services, monetary allowances, and survivor benefits.

e. Assist Code 10A in maintaining an accurate and comprehensive survivor benefits information package.

f. Maintain a list of current FLOs and maintain operational control of the program.

g. Establish an MOU with JPED designed to receive, safeguard, and determine final disposition of personal effects of all casualty, serious injury, or EAWUN personnel.

h. Assist survivors in navigating the system of benefits and monitor each casualty, EAWUN, or SI situation to ensure survivors are provided with information and assistance for as long as needed.

i. Be a member of the CWG and assist all aspects of the CWG to ensure next of kin receive information and assistance as long as needed.

j. Upon notification of a casualty, assist next of kin with support from like-minded organizations and support groups (e.g., Concerns of Police Survivors (COPS)).

50-15.5. Assistant Director for Communications (Code 00C) shall:

a. Participate as a member of the CWG upon implementation.

b. Develop and plan for official honors at a funeral.

50-15.6 General Counsel (00L) shall participate as a member of the CWG upon implementation.

50-15.7. Chief Psychologist, Behavioral Sciences (02D) shall participate as a member of the CWG upon implementation.

50-15.8. The Chief Intelligence and Information Sharing (Code 25) shall:

a. Ensure MTAC/Law Enforcement Desk personnel are trained and have access to TRACES.

b. Ensure MTAC personnel provide support by accessing and monitoring TRACES during a casualty or serious injury.

50-15.9 Family Liaison Officer

a. Perform as a primary duty the rendering of assistance to the next of kin designated on the DD FORM 93, which will include informing them of survivor and other benefits which may be available, assisting with the completion and filing of claim forms, and ensuring benefits are received.

b. The FLO assistance process can be broken into phases:

(1) Phase I: Notification and Condolence Phase. The FLO may be asked to accompany a NCIS senior leader to the initial notification of the next of kin. The purpose of this visit is to provide the initial notification of the serious injury, EAWUN, or casualty, provide any factual background information available, and (as appropriate) offer condolences on behalf of NCIS. Appendix B will be used to guide the FLO and senior leader making next of kin notification.

(2) Phase II: Disposition of Remains/Medical Evacuation of Patient. During this phase, the FLO will assist the next of kin in tracking the patient or remains from the place of the casualty to the appropriate hospital or funeral home. Entitlements for this phase will depend upon the circumstances and location of the incident.

(3) Phase III: Completion of Entitlements and Benefits Claim Forms. The FLO will assist the next of kin in obtaining, completing, and filing all appropriate claim forms to ensure the next of kin receive all the entitlements and benefits dictated by the situation.

(4) Phase IV: Follow Up. The FLO will stay in touch with the next of kin to ensure all entitlements and benefits are received and that any additional issues (within the purview of NCIS and the FLO) are resolved. This phase will typically last 60 days, at which time the FLO will coordinate with the CAP Manager to determine how and when to transition the next of kin to long term care.

APPENDIX A: Record of Emergency Data DD Form 93

RECORD OF EMERGENCY DATA

PRIVACY ACT STATEMENT

AUTHORITY: 5 USC 552, 10 USC 655, 1475 to 1480 and 2771, 38 USC 1970, 44 USC 3101, and EO 9397 (SSN).
PRINCIPAL PURPOSES: This form is used by military personnel and Department of Defense civilian and contractor personnel, collectively referred to as civilians, when applicable. **For military personnel,** it is used to designate beneficiaries for certain benefits in the event of the Service member's death. It is also a guide for disposition of that member's pay and allowances if captured, missing or interned. It also shows names and addresses of the person(s) the Service member desires to be notified in case of emergency or death. **For civilian personnel,** it is used to expedite the notification process in the event of an emergency and/or the death of the member. The purpose of soliciting the SSN is to provide positive identification. All items may not be applicable.
ROUTINE USES: None.
DISCLOSURE: Voluntary; however, failure to provide accurate personal identifier information and other solicited information will delay notification and the processing of benefits to designated beneficiaries if applicable.

INSTRUCTIONS TO SERVICE MEMBER

This extremely important form is to be used by you to show the names and addresses of your spouse, children, parents, and any other person(s) you would like notified if you become a casualty (other family members or fiance), and, to designate beneficiaries for certain benefits if you die. IT IS YOUR RESPONSIBILITY to keep your Record of Emergency Data up to date to show your desires as to beneficiaries to receive certain death payments, and to show changes in your family or other personnel listed, for example, as a result of marriage, civil court action, death, or address change.

INSTRUCTIONS TO CIVILIANS

This extremely important form is to be used by you to show the names and addresses of your spouse, children, parents, and any other person(s) you would like notified if you become a casualty. Not every item on this form is applicable to you. **This form is used by the Department of Defense (DoD) to expedite notification in the case of emergencies or death.** It does not have a legal impact on other forms you may have completed with the DoD or your employer.

IMPORTANT: This form is divided into two sections: Section 1 - Emergency Contact Information and Section 2 - Benefits Related Information. READ THE INSTRUCTIONS ON PAGES 3 AND 4 BEFORE COMPLETING THIS FORM.

SECTION 1 - EMERGENCY CONTACT INFORMATION

1. NAME *(Last, First, Middle Initial)*	2. SSN

3a. SERVICE/CIVILIAN CATEGORY	b. REPORTING UNIT CODE/DUTY STATION
☐ ARMY ☐ NAVY ☐ MARINE CORPS ☐ AIR FORCE ☐ DoD ☐ CIVILIAN ☐ CONTRACTOR	

4a. SPOUSE NAME *(If applicable) (Last, First, Middle Initial)*	b. ADDRESS *(Include ZIP Code)* AND TELEPHONE NUMBER
☐ SINGLE ☐ DIVORCED ☐ WIDOWED	

5. CHILDREN a. NAME *(Last, First, Middle Initial)*	b. RELATIONSHIP	c. DATE OF BIRTH *(YYYYMMDD)*	d. ADDRESS *(Include ZIP Code)* AND TELEPHONE NUMBER

6a. FATHER NAME *(Last, First, Middle Initial)*	b. ADDRESS *(Include ZIP Code)* AND TELEPHONE NUMBER

7a. MOTHER NAME *(Last, First, Middle Initial)*	b. ADDRESS *(Include ZIP Code)* AND TELEPHONE NUMBER

8a. DO NOT NOTIFY DUE TO ILL HEALTH	b. NOTIFY INSTEAD

9a. DESIGNATED PERSON(S) *(Military only)*	b. ADDRESS *(Include ZIP Code)* AND TELEPHONE NUMBER

10. CONTRACTING AGENCY AND TELEPHONE NUMBER *(Contractors only)*

DD FORM 93, JAN 2008 PREVIOUS EDITION IS OBSOLETE. Adobe 7.0 Professional

APPENDIX B: Emergency Notification Protocol

Emergency Notification Protocol

In the event an NCIS employee is seriously injured, dies or is declared missing, the following actions will be taken:

1. Post-Incident Notification

a. Senior on-scene or NCIS employee with official knowledge of the situation notifies MTAC at (b)(6) Report on:

(1) Employee name

(2) Incident details

(3) Injuries sustained

(4) Condition of personnel involved

(5) Location of personnel or decedent(s)' remains

(6) Follow up with written confirmation (email, facsimile, or message) of the incident

(7) Provide updates as new information becomes available

b. MTAC Watch contacts:

(1) DAD, MTAC or next senior NCIS manager of the MTAC

c. DAD, MTAC or MTAC Watch, if unable to notify MTAC management, notifies:

(1) Chief of Staff

(2) DAD/SAC at the employee's permanent duty station

(3) SAC, CRFO if incident happens to a deployed NCIS member

(4) Commanding Officer, Office of Military Support (OMS) if NCIS employee is an active duty or reserve military member

(5) AD HR (Code 10)

(6) Inspector General (Code 00I)

(7) Assistant Director for Communications (Code 00C)

d. Chief of Staff notifies:

(1) Director NCIS

(2) Deputy Director

(3) Principal Executive Assistant Director M&A

(4) Operational EAD as appropriate

(5) NCIS Representative to the Navy Staff

e. SAC/DAD contacts Family Liaison Officer (FLO) and appropriate admin staff to determine location of casualty's next of kin.

(1) If next of kin are located away from casualty's permanent duty station, SAC/DAD notify SAC of closest field office to make in-person notification.

f. SAC/DAD, FLO, make official family notification.

g. SAC notifies Director NCIS, Chief of Staff, and MTAC that family has been notified.

h. Director NCIS contacts family.

i. FLO contacts CAP Manager to coordinate benefits and provide follow-up support as required by next of kin (NOK).

j. SAC/DAD draft "Death in the NCIS Family" GEN Admin (in the event of death) and forward to Code 00C for coordination and release.

2. Notification Considerations. Notification will be made by the SAC/DAD or most senior NCIS representative on-scene to the person(s) identified by the employee as NOK during pre-deployment interview or on the emergency notification/personal data form. The following procedures apply:

a. Unless the situation dictates otherwise (e.g. potential for media to break story that leaves little doubt as to identity of employee), do not make notifications before 0600 and after 2300 local time, but do not otherwise delay notification.

b. Do not release employee's identity to the news media. Refer all press or public inquiries to the Communications Directorate (Code 00C).

c. All measures should be taken to ensure the notification takes place in person.

d. Try to gather the adults present and sit them down.

e. Slowly and clearly inform them of the available information. Inform the family of the date, time, and circumstances surrounding the NCIS employee's missing status, injury or death except when that information would hinder ongoing operations and/or investigations as they relate to the health, safety and welfare of others.

f. If employee has died, inform the person(s) of the death using employee's name and the terms "died" or "death".

g. Never give the person(s) a false sense of hope and be truthful.

h. If the employee is at a local hospital and the person(s) notified wants to go to the hospital, provide transportation if feasible.

i. Discourage family members from driving themselves to the hospital.

j. If requested by person(s) being notified:

(1) Contact other family members.

(2) Assist in arranging childcare, and if necessary, alternate lodging.

k. Inform next of kin that an NCIS representative will be made available to assist the family. Provide identity if known.

l. Each SAC may coordinate with the Military Chaplain Officer (MCO) aboard their base to identify civilian counterparts in the community who are trained and willing to assist NCIS in the notification process. The MCO and/or the civilian chaplain/minister/priest may be available to assist NCIS when delivering death, serious injuries, or missing status notification to next of kin. Additionally, the MCO or the minister or priest can assist the next of kin and family in the grieving and emotional healing process with psychological, emotional and religious support. The MCO/minister/priest can be a helpful member of the notification process because the MCO/minister/priest may likely have an increased level of experience assisting family members and loved ones dealing with grief and loss.

APPENDIX C: NCIS Form 12295/1 (Jul 2010)

Line of Duty Death/Serious Injury Notification

PII Statement:

NOTE: This form is voluntary. Information you choose to provide here will only be utilized to assist NCIS in the processes of notifying and assisting your next of kin in the event of your critical injury or death while you are performing your job related duties (Line-of-Duty). If you choose to fill it out, please take the time to complete each item accurately to ensure your next of kin is afforded the appropriate assistance. Please attach additional information as needed. ONCE COMPLETE, PLEASE SEAL IN AN ENVELOPE WITH YOUR NAME ON THE OUTSIDE AND RETURN TO POINT OF CONTACT RESPONSIBLE FOR SAFEKEEPING THIS INFO IN YOUR OFFICE.

Section A: Personal Information

1. Name: _____
Last First MI

2. Address:
_____
Street Address (Not P.O. Box)

_____
City State Zip Code

3. Telephone:
_____
Home Cell

4. Medical Insurance:
_____
Provider Name Policy Number

5. Medical Conditions/Allergies:
_____

_____

_____

6. Religion:

_____

7. Name of Clergy Member:

_____
First Last

8. Address:

_____
Street

_____
City State Zip Code

9. In the event of death or serious injury, would you like this clergy member to accompany the NCIS representative during notification of your next of kin?
☐ Yes ☐ No

Section B: Family Information

1. Spouse

a. Spouse: _____
Last First MI Preferred Name

b. Address:

_____
Street

_____
City State Zip Code

c. Phone: _____
Home Cell

d. Spouse Employer:

_____
Name

e. Employer Address: _____
Street Address

_____

City State Zip Code

f. Phone at Work:

_____

2. Children (Who Reside with You)

a. Name: _____
First MI Last Preferred Name Date of Birth

School/Work:

_____
Name Address Phone

b. Name: _____
First MI Last Preferred Name Date of Birth

School/Work:

_____
Name Address Phone

c. Name: _____
First MI Last Preferred Name Date of Birth

School/Work:

_____
Name Address Phone

d. Name: _____
First MI Last Preferred Name Date of Birth

School/Work:

_____
Name Address Phone

e. Name: _____
First MI Last Preferred Name Date of Birth

School/Work:

_____
Name Address Phone

f. Name:

_____
First MI Last Preferred Name Date of Birth

School/Work:

_____

Name Address Phone

---

3. Other Dependents Who Reside With You

a. Name:

_____

First MI Last Preferred Name Date of Birth

School/Work:

_____

Name Address Phone

b. Name:

_____

First MI Last Preferred Name Date of Birth

School/Work:

_____

Name Address Phone

c. Name:

_____

First MI Last Preferred Name Date of Birth

School/Work:

_____

Name Address Phone

---

4. Pets

a. _____

Type Quantity Names

b. _____

Type Quantity Names

---

5. Key Relatives (Who Don't Reside with You)

ONLY complete IF you want a NCIS representative to contact in the event of critical injury or death.

a. Name:

_____

Last First MI Preferred Name

Address:

_____

Street

_____

City State Zip Code

Phone:

_____

Home Work Cell

b. Name:

_____

Last First MI Preferred Name

Address:

_____

Street

_____

City State Zip Code

Phone:

_____

Home Work Cell

c. Name:

_____

Last First MI Preferred Name

Address:

_____

Street

_____

City State Zip Code

Phone:

_____

Home Work Cell

---

6. Former Spouse (ONLY complete IF you want a NCIS representative to contact in the event of critical injury or death)

Name:

_____

Last First MI Preferred Name

Address:

_____

Street

_____

City State Zip Code

Phone:

_____

Home Work Cell

Section C: Notification Process

1. Is there anyone you would like to accompany the NCIS representative when notification is made to your immediate family (include address and phone number)?

2. Is there anyone you would like notified to assist your family in the aftermath (include address and phone number)?

3. Is there anyone you wish NOT to be involved in the notification of your immediate family regarding death or serious injury?

4. Is there any additional information or health issues that may require special assistance during notification of a specific person (include name and specific requirements/issues, for example, heart condition, serious illness, etc.)?

5. Are there any special requests regarding your funeral service (police funeral, military funeral, etc.)?

6. Please list the person authorized to direct disposition of your remains (this individual is referred to as a PADD (Person Authorized to Direct Disposition) in DoD casualty instructions and is authorized to specify where remains are sent--**this designation is optional for civilians**.

7. Please list the person eligible to receive your personal effects (this individual is referred to as a PERE (Person Eligible to Receive Personal Effects) in DoD casualty instructions and will receive any personal effects recovered in the event of a casualty or serious injury).

8. Please provide any other information that will assist NCIS in the notification process or in caring for your family in the event of your serious injury or death.

NCIS-1, CHAPTER 51
AGREEMENTS
EFFECTIVE DATE: AUGUST 2014

TABLE OF CONTENTS **PAGE**

51-1. Purpose

a. This chapter establishes policy to initiate, staff, and obtain required approvals prior to entering into an agreement with another party in accordance with the references listed in Appendix A. The parties to an agreement (Memorandum of Agreement (MOA), Memorandum of Understanding (MOU), or an Inter-Service Support Agreement (ISSA)) covered by this chapter are NCIS and one or more governmental or private entities.

b. This chapter applies to all unclassified and classified agreements and to all NCIS employees and contractor personnel who draft an agreement.

c. This chapter does not address international agreements. Agreements effected under this chapter are not appropriate instruments for international agreements. Reference (a) contains guidance for international agreements.

51-2. Policy

a. NCIS offices and representatives are required to coordinate the review of draft agreements with NCIS Headquarters prior to signing or entering into an agreement.

b. Recurring support and cooperation with city, county, State, and Federal Government entities, and with non-profit organizations that do not require reimbursement (no cost) should be documented with an agreement. An agreement may be used to document mutual understanding of facts, intentions, procedures, limits on future actions, areas of present or future coordination, or commitments.

c. Recurring interservice and intragovernmental support that requires reimbursement must be documented on DD Form 1144, "Support Agreement." References (b) and (c) identify requirements and guidelines of interservice and intragovernmental support agreements.

51-3. Cancellation. NCIS-1, Chapter 51, Agreements, dated March 2011.

51-4. Chapter Sponsor. The sponsor of this chapter is the Administrative Services Department (Code 11C).

51-5. Definitions

a. Memorandum of Agreement (MOA). A document that details the specific responsibilities of, and actions to be taken by, each of the parties so that their goals may be accomplished. An MOA may also indicate the goals of the parties to help explain their actions and responsibilities.

b. Memorandum of Understanding (MOU). A document that describes very broad concepts of mutual understanding, goals, and plans shared by the parties.

c. Inter-Service Support Agreement (ISSA). Action by one Military Service or element thereof to provide logistic and/or administrative support to another Military Service or element thereof. Such action may be recurring or nonrecurring in character on an installation, area, or worldwide basis.

51-6. Responsibilities

a. Executive Assistant Directors (EADs) and Assistant Directors (ADs) will monitor their directorates and field activities to facilitate compliance with chapter requirements. EADs and ADs must approve draft agreements for NCIS Headquarters review prior to submission to Code 11C for staffing.

b. Special Agents in Charge (SACs), Deputy Assistant Directors (DADs), and heads of the Director's immediate staff offices (Senior Adviser, Director of Communications, Inspector General, and Counsel) work closely with their departments and field offices to facilitate compliance with chapter requirements. SACs, DADs, and heads of the Director's immediate staff must approve draft agreements, in accordance with the template provided in Appendix B, for NCIS Headquarters review prior to submission to Code 11C for staffing. Appendix C is provided as a checklist to assist in the submission of draft agreements.

c. The Administrative Services Department (Code 11C) will serve as the Support Agreement Manager, central collection point, and cross-functional facilitator for staffing NCIS agreements. Code 11C is responsible for:

(1) Monitoring the preparation of support agreements and facilitating coordination and approvals.

(2) Administering NCIS' support agreements as directed by Director, NCIS.

(3) Maintaining a master record of active agreements. The master record will include one signed and dated copy provided by the NCIS sponsor of the agreement.

(4) Processing the draft agreement submitted by the NCIS sponsor for NCIS Headquarters review and approval decision.

(5) Staffing draft agreements to the Secretary of the Navy's office and appropriate DoD staff offices as required by the applicable Department of the Navy (DON) and DoD issuances.

d. The NCIS sponsor of the agreement (originating office) is required to:

(1) Submit a complete staffing package to Code 11C for NCIS Headquarters review and approval decision.

(2) Coordinate with the agreement party(ies) to obtain final signatures once NCIS Headquarters approval is obtained and documented.

(3) Maintain an official record copy of the agreement once all parties have signed.

(4) Provide one signed and dated copy of the agreement to Code 11C for the master record of active agreements.

(5) Review agreements every three years or earlier based on the terms of the agreements to determine whether they are current and in effect, expired, canceled, or require updating. EADs, ADs, DADs, and SACs should conduct reviews signed by their predecessors during turnovers.

(6) Submit one of the following items to Code 11C, based on the outcome of the review:

(a) Email confirmation, using the template provided in Appendix D, that the agreement is current, in effect, and requires no update.

(b) Email the updated agreement and complete staffing package for NCIS Headquarters review. See paragraph 51-11 for staffing package requirements.

(c) Email confirmation, using the template provided in Appendix E, that the agreement has been terminated or has expired.

51-7. Limitations

a. Each agreement must be consistent with the NCIS mission and conform to Federal law, regulations, and funding constraints. Additionally, the existence of an agreement does not eliminate or diminish the need for additional contracts, documents, or agreements to execute the activities contemplated by the parties. Neither this section nor any agreement may be used as the sole authority or means to acquire or procure goods or services, exchange funds or property, or transfer or assign personnel. Although the agreement can address those issues and indicate the goals and intent of the parties, all NCIS personnel must comply fully with pertinent contracting and procurement regulations and human resources or program requirements and regulations.

b. Agreements may address the following special situations, but they may not be used as the sole means to effect agreements or actions. The sponsor should review the following references for authority when creating an agreement.

(1) Review reference (d) when developing an agreement to detail NCIS personnel to duty outside the DoD. The following are highlights contained in reference (d).

(a) As a general policy, DoD will approve requests for details outside the Department only on a reimbursable basis.

(b) Non-reimbursable personnel details will be executed only if the employee will be performing functions consistent with those for which DoD funds are appropriated and the greatest benefit of the detail accrues to the DoD. The external duties will relate to matters ordinarily handled by the DoD and the Department in accomplishing its functions. Details may be beneficial to both agencies, but absent a clear showing of preponderant benefit accruing to the DoD, approval will be on a reimbursable basis.

(c) Personnel will not be detailed outside the DoD when such a detail would be the individual's final tour before retirement or separation.

(d) Agreements detailing NCIS personnel outside of DoD must be reviewed by NCIS Headquarters and the Director of Administration and Management, OSD, via the Under Secretary of the Navy. A sample action memo, sample request for detail format, and a sample statement of duties are provided in Appendix F.

(2) Review reference (e) when developing agreements regarding staffing at U.S. embassies that require Deputy Under Secretary of the Navy (Plans, Policy, Oversight, and Integration) review and approval.

(3) Review references (f) when considering an agreement that impacts intelligence, counterintelligence, and other sensitive activities sponsored or conducted by Governmental agencies.

(4) Review reference (g) when developing an agreement with other DoD components specifying tailored counterintelligence support to be provided.

(5) Review reference (h) when considering personnel for assignment to a Joint Intelligence Community Duty Assignment.

(6) Review reference (i) when considering developing an agreement on proposed defense human intelligence and related intelligence activities.

(7) Review reference (j) for other useful information relating to existing agreements between DoD, DON, and other Federal Government agencies.

c. Assessment Statement. The NCIS sponsor of the agreement will complete and submit the required assessment statement for staffing. An assessment statement template is provided as Appendix G. The assessment standards are based on criteria contained in DON policy, specifically reference (k). The NCIS Headquarters departments and counsel staff will review each agreement to determine whether external coordination by DoD and/or DON is required. Positive responses to any of the questions below require a justification statement within the assessment statement and may result in external review by DoD and/or DON offices.

(1) Does the agreement have the potential for public controversy or embarrassment, either domestically or overseas?

(2) Does the agreement have the potential to create unusual or significant risks to DON property and/or personnel?

(3) Does the agreement have the potential to cause adverse foreign military or diplomatic reactions or consequences?

(4) Does the agreement have the potential for negatively affecting DON relations with, or support to, other Military Departments or Government agencies?

(5) Does the agreement contain DON-wide issues and DON-wide relations with, or support to, other Military Departments or Government agencies?

(6) Does the agreement assign NCIS special agents outside of DoD?

51-8. Prohibited Indemnification Agreements or Clauses. An agreement to indemnify is an agreement to assume financial, legal, or other liabilities on behalf of the other party. Neither the NCIS nor any person in NCIS may agree to indemnify any other party absent specific Federal statutory authorization and approval. Federal law, 31 U.S.C. sections 1341(a)(1)(A) and 1341(a)(1)(B), commonly referred to as the Anti-Deficiency Act, prohibits all officers and employees of the United States from making or authorizing expenditures or obligations exceeding appropriated funding and from obligating payment of money before it is appropriated. A typical indemnification clause violates both provisions of that Act because it potentially obligates the Federal Government (or NCIS) to pay an unspecified, unlimited, or unappropriated amount of money if someone else's property is lost, damaged or destroyed; if a person is injured or killed; or other parties to the agreement incur legal liabilities or expenses. If a prospective

party to an agreement requests or demands that the NCIS agree to an indemnification clause, contact NCIS Counsel (Code 00L) for assistance.

51-9. Review and Approval

a. All agreements must be reviewed and approved for signature at the appropriate level. Early coordination and communication with interested offices and editing of a draft agreement with the other party is encouraged.

b. The NCIS sponsor will ensure that the draft agreement does not conflict with any preexisting agreements prior to submission to Code 11C for staffing. To see current agreements, go to Lighthouse and click on the Publications tab and navigate to the Agreements page.

c. The NCIS Headquarters review and approval process may take 30 days or more, depending on reviewer comments and edits requiring resolution. The NCIS sponsor will plan accordingly for the staffing process. Expedited staffing requests will be accompanied with justification and an impact statement if the deadline is not met.

51-10. Language Requirements

a. If an agreement is deemed appropriate for an activity, determine whether a current agreement addresses the issues of mutual interest and can be modified or updated to address the mutual concerns. If no relevant agreement exists, draft a new agreement following the guidelines in paragraph 51-11 and Appendix B.

b. The NCIS sponsor of the agreement must ensure the document is properly constructed and coordinated.

c. If an agreement is initiated by a non-DoD activity, NCIS is authorized to use that activity's format, but the provisions of the format must address the required areas of concern in this chapter.

51-11. Format Requirements. The structure of an agreement drafted by NCIS is shown in Appendix B. The wording of the agreement may be changed to reflect multiple parties. Appendix B may be tailored to accommodate the subject matter of the agreement, the needs of the parties, or to conform to an applicable law, regulation, or directive. If a party other than NCIS originates the agreement, that template may be used and accepted. All agreements must include the following information:

a. Purpose. Clearly state the purpose or reason for entering into the agreement.

b. Parties. Identify the parties to be bound by the agreement.

c. Authority. Cite the legal authority for the agreement. Reference all applicable Federal regulations, DoD directives and instructions, SECNAV instructions, or other directives.

d. Responsibilities. Include a description of the duties and responsibilities of the parties. The description should be as specific and detailed as necessary. Other pertinent details may be provided in an appendix rather than the body of the agreement.

e. Reporting and Documentation. Specify whether follow up reports or documentation of actions taken are required. State how often, and to whom, follow up reports must be submitted.

f. Points of Contact. Identify the agreement points of contact for all parties, including names, position title, office symbols, addresses, and phone numbers.

g. Other Provisions. If applicable and appropriate, after all other administrative permissions are granted regarding personnel assignment or detailing, set forth the parties' obligations regarding pay, overtime, travel, office support, evaluations, etc. See Appendix H for examples.

h. Modification. Include a provision stating how to amend the agreement. While it is often appropriate for those at the working level to make modifications, either orally or in writing, modifications that change central provisions of the agreement must be made in writing and submitted to NCIS Headquarters for review. Appendix I provides a template for addendum.

i. Effective Date. Identify the date the agreement becomes effective. This may be a specific date after the agreement is signed by all parties or the date the last party signs the agreement.

j. Review. Include language to state how often the agreement will be reviewed. In accordance with reference (b), DoD Components must review support agreements at least triennially in its entirety and document each review. Appendix D provides a review template.

k. Termination. In accordance with guidance provided in reference (b), include statements or provisions for termination of the agreement. The document must indicate that it will terminate on a certain date, upon the accomplishment of its purpose, or upon agreement of the parties, not to exceed nine years. The agreement must also contain a provision indicating whether the duration of the agreement may be extended and, if so, the extension mechanism (by written agreement of the parties). Finally, the agreement must indicate whether a party may terminate the agreement early (usually by written notice to the other parties).

l. Approving Official

(1) NCIS is party to the agreement, not the person signing for NCIS. Therefore, that person must have the authority to sign the agreement and commit NCIS. In determining who that official is, refer to the statute, regulation, or directive authorizing NCIS participation in the agreement. Even if the authority to sign an agreement has been delegated to a SAC, if a Uniformed Service Chief or Agency Head is signing for another party, it may be appropriate for the NCIS Director or Deputy Director to sign as a matter of protocol.

(2) In accordance with reference (b), approval authority signatures must never appear alone on a blank page; the signature page must contain text from the agreement.

(3) All agreements must be signed by the SAC/AD level or higher.

51-12. Staffing Requirements and Process

a. The NCIS sponsor of the agreement is responsible for submitting the staffing package to Code 11C via the appropriate group email address.

(1) Unclassified. (b)(7)(E) @navy.mil.

(2) Classified. (b)(7)(E) @ncis.navy.smil.mil.

b. The staffing package must include the draft agreement (MOA, MOU, or ISSA), completed assessment statement, completed blazer, and EAD or AD (Headquarters) or SAC (field office) approval. Enclosures to the agreement, references, or supporting documentation must be submitted to facilitate review. Word documents are strongly recommended and will enable edits or comments to be inserted efficiently during the NCIS Headquarters review.

c. All agreements submitted to Code 11C will be entered into the Taskers System for staffing and assigned a tasker document control number for tracking purposes. The NCIS sponsor (HQ code or field office) will be granted access to the tasker for monitoring status, entering comments, editing documents, etc.

d. At a minimum, agreements will be staffed to the appropriate program management office, Inspector General, Counsel, and the Chief of Staff for coordination and concurrence or non-concurrence comments. The DAD, Code 11C, may grant exemptions to the staffing workflow on a case-by-case basis.

e. If the agreement is approved for signature, the NCIS sponsor is responsible for coordinating with the other party(ies) for final signatures. The NCIS sponsor is responsible for submitting a signed and dated copy of the agreement to Code 11C for retention. Code 11C will post the final signed agreement (if unclassified) to Lighthouse and maintain a copy in the agreement master files.

f. Agreement records created as a result of this chapter, regardless of media, will be managed in accordance with reference (l).

APPENDIX A
REFERENCES

(a) DoD Directive 5530.3, International Agreements, 11 June 1987, Certified Current as of 21 November 2003

(b) DoD Instruction 4000.19, Support Agreements, 25 April 2013

(c) OPNAV Instruction 4000.84C, Support Agreements, 31 May 2012

(d) DoD Instruction 1000.17, Detail of DoD Personnel to Duty Outside the Department of Defense, 30 October 2013

(e) SECNAV Instruction 1300.15, National Security Decision Directive 38, 24 January 2013

(f) DoD Directive S-5210.36, Provision of DoD Sensitive Support to DoD Components and Other Departments and Agencies of the U.S. Government (U), 6 November 2008

(g) DoD Instruction 5240.10, Counterintelligence (CI) in the Combatant Commands and Other DoD Components, Incorporating Change 1, 15 October 2013

(h) DoD Instruction 1400.36, DoD Implementation of the Joint Intelligence Community Duty Assignment (JDA) Program, 2 June 2008

(i) DoD Instruction S-5200.42, Defense Human Intelligence (HUMINT) and Related Intelligence Activities (U), Incorporating Change 1, 16 August 2010

(j) NAVSO P-1000, Department of the Navy Financial Management Policy Manual, 12 December 2002

(k) SECNAV Instruction 5000.34E, Oversight and Management of Intelligence Activities, Intelligence-Related Activities, Special Access Programs and Sensitive Activities Within the Department of the Navy, 17 May 2012

(l) SECNAV M-5210.1, Department of the Navy Records Management Manual, Incorporating Change 1, May 2012

APPENDIX B
AGREEMENT TEMPLATE

MEMORANDUM OF AGREEMENT/UNDERSTANDING
BETWEEN
THE NAVAL CRIMINAL INVESTIGATIVE SERVICE
AND
[INSERT OTHER PARTY(IES)/ORGANIZATION]

5700
[Insert NCIS sponsor's serial number]

Subj: [INSERT TEXT]

Ref: (a) [Cite the legal authorities for the agreement and other appropriate references]

1. Purpose. The purpose of this agreement is to set forth terms by which [insert text] and [insert text] will provide [services, personnel, equipment] in order to [summarize what the Agreement is intended to accomplish].

2. Parties. The parties to this agreement are the Naval Criminal Investigative Service (NCIS) and [insert text].

3. Authority. Cite the legal authority for the agreement. Reference all applicable Federal regulations, DoD directives and instructions, SECNAV instructions, and other directives.

4. Responsibilities

a. NCIS

(1) [Describe what NCIS will do. Include a paragraph indicating whether NCIS is required to submit status or progress reports and, if so, how often].

(2) [Add subparagraphs as needed].

b. [Insert the other party's name]

(1) [Describe the other party's responsibilities, as discussed above].

(2) [Add subparagraphs as needed].

APPENDIX B: (CONTINUED)
AGREEMENT TEMPLATE

5. Reporting and Documentation

[Delete this section if it is not needed to document follow up reports or actions taken].

6. Points of Contact

a. NCIS [Identify points of contact for NCIS and the other party, including office symbol, address, and phone number (fax number and email or Internet addresses may also be included)].

b. [Insert the other party's contacts.]

7. Other Provisions

a. Nothing in this agreement is intended to conflict with current law or regulation or the directives of the DoD, DON, or NCIS. If a term of this agreement is inconsistent with such authority, then that term will be invalid, but the remaining terms and conditions of this agreement will remain in full force and effect.

b. This agreement does not obligate funds and will not be used to obligate or otherwise commit funds or serve as the basis for the transfer of funds. Implementation of this agreement is subject to the availability of funds. Detailed and coordinated instructions amplifying the terms of this agreement may be published by the parties if deemed necessary.

c. This agreement is not intended, and should not be construed, to create any right or benefit, substantive or procedural, enforceable at law or otherwise by any party against the parties, their parent agencies, the United States, or the officers, employees, agents, or other associated personnel thereof.

d. If applicable and appropriate, after all other administrative permissions are granted regarding personnel assignment or detailing, set forth the parties' obligations regarding pay, overtime, travel, office support, evaluations, etc. See Appendix H for other useful template information.

8. Modification. This agreement may be modified upon the mutual (written) consent of the parties. See Appendix I for an addendum template.

9. Effective Date. The terms of this agreement becomes effective on [insert effective date]. This MOU takes effect beginning the day after the last party signs.

10. Review. This document will be reviewed in its entirety [annually, biannually, or triennially]. Review will be initiated by [name of responsible party]. See Appendix D for an annual review template.

APPENDIX B: (CONTINUED)
AGREEMENT TEMPLATE

11. Termination. The terms of this agreement, as modified with the consent of both parties, will remain in effect until [date, completion of project, or upon agreement of parties]. The agreement may be extended by mutual written agreement of the parties. Either party upon [number] days' written notice to the other party may terminate this agreement.

APPROVED BY:

_____
[Name of NCIS signatory]
[Position/Title]
Naval Criminal Investigative Service

Date Signed: _____
MM/DD/YYYY

APPROVED BY:

_____
[Name of other party's signatory]
[Position/Title]
[Other party's organization]

Date Signed: _____
MM/DD/YYYY

APPENDIX C
AGREEMENT CHECKLIST

✓ **ALL** agreements **MUST** be routed to NCIS Headquarters Front Office for approval **PRIOR** to signing.

✓ The other party's format may be used; however, ensure the mandatory NCIS verbiage and paragraphs are included.

✓ Font is 12-point Times New Roman.

✓ Use "Ref:" to cite the legal authorities for the agreement. Verify that cited legal authorities are current.

✓ 1. Purpose. Mandatory paragraph.

✓ 2. Parties. Mandatory paragraph.

✓ 3. Authority. Mandatory paragraph.

✓ 4. Responsibilities. Mandatory paragraph and subparagraphs. a. NCIS b. [Other party].

✓ 5. Reporting and Documentation. Mandatory if NCIS or the other party requires follow up reports or documentation of actions taken.

✓ 6. Points of Contact. Mandatory paragraph and subparagraphs. a. NCIS b. [Other party]. Name, office symbol, address, phone number, fax number, and email, as needed.

✓ 7. Other Provisions. Mandatory subparagraphs a., b., and c.

✓ 8. Modification. Mandatory paragraph.

✓ 9. Effective Date. Mandatory paragraph.

✓ 10. Review. Mandatory paragraph, must be reviewed at least every three years.

✓ 11. Termination. Mandatory paragraph, timeframe is not to exceed nine years.

✓ 12. Approved by/Signature block. Mandatory paragraph that must not be placed on a page without text. Ensure names and dates are typed or printed legibly.

✓ 13. A completed Assessment Statement must be submitted with each agreement.

✓ 14. A completed green blazer must be submitted with each agreement. A package will not be staffed if block 13, paragraphs 1, 2, 3, and 4 of the green blazer are not completed.

APPENDIX D
AGREEMENT ANNUAL REVIEW TEMPLATE

MEMORANDUM OF AGREEMENT/UNDERSTANDING – ANNUAL REVIEW
BETWEEN
NAVAL CRIMINAL INVESTIGATIVE SERVICE
AND
NAME/TITLE OF OTHER AGENCY/UNIT/COMMAND

Subj: MEMORANDUM OF UNDERSTANDING – ANNUAL REVIEW FOR ORIGINALLY TITLED MOU

Ref: (a) Original Agreement

1. Purpose. To conduct the annual/bi-annual/tri-annual review of reference (a), as required.

2. Background. Name/Title of other Agency/Unit/Command entered into reference (a) with NCIS on date of original Agreements.

3. Review. Reference (a) has been reviewed in its entirety and it will remain in effect as written.

_____
[Name of NCIS signatory] MM/DD/YYYY
[Position/Title]
Naval Criminal Investigative Service

APPENDIX E
AGREEMENT TERMINATION TEMPLATE

MEMORANDUM OF AGREEMENT/UNDERSTANDING – TERMINATION OF AGREEMENT
BETWEEN
NAVAL CRIMINAL INVESTIGATIVE SERVICE
AND
NAME/TITLE OF OTHER AGENCY/UNIT/COMMAND

Subj: MEMORANDUM OF UNDERSTANDING – TERMINATION OF AGREEMENT FOR ORIGINALLY TITLED AGREEMENT

Ref: (a) Original Agreement

1. Purpose. To terminate the agreement of reference (a) as required.

2. Background. Name/Title of other Agency/Unit/Command entered into reference (a) with NCIS on date of original agreement.

3. Review. Reference (a) has been reviewed in its entirety and is no longer valid/necessary/ required as written.

4. Effective Date. This memorandum of agreement termination becomes effective the date signed by all parties listed in this agreement.

_____	_____
[Name of NCIS signatory] MM/DD/YYYY	[Other party's signatory] MM/DD/YYYY
[Position/Title]	[Position/Title]
Naval Criminal Investigative Service	[Other party's organization]

APPENDIX F
DETAIL OF DOD PERSONNEL TO DUTY OUTSIDE OF DOD REQUEST TEMPLATE

All packages must contain an Action Memo, Detail Format, and Statement of Duties.

1. Action Memo to the Director. Refer to NCIS-1, Chapter 3, Executive Decision Making Process.

2. Request for Detail Format. This document will be an attachment to the Action Memo as TAB A:

"MEMORANDUM FOR UNDER SECRETARY OF THE NAVY
%
Subject: Request for Detail of Personnel Outside the Department of Defense
%
We request approval to [detail, replace, or extend] a position in the office of [complete title or office] on a [reimbursable, non-reimbursable] basis for a period of [time in months or years]. A Statement of Duties is attached. The detail will be in accordance with the provisions of DoD Instruction 1000.17, Detail of DoD Personnel to Duty Outside of the Department of Defense.
%
If you have any questions about this request, please contact [Insert Name, Office, phone number, (email address)].
%

(Leave blank)

%
Attachment:
Statement of Duties

3. Statement of Duties. This document will be an attachment to the Action Memo as TAB B:

"Naval Criminal Investigative Service Point of Contact: [*Leave blank*]

1. Name of Person (Detail): [Insert name if requesting an extension of an existing detail; otherwise leave blank].

2. Position Title: [Insert position title].

3. Position Location: [Insert duty location, street address].

4. Requested Military Rank/Civilian Grade: [Required; do not leave blank].

5. DoD Agency or Branch of Service: [Insert specific DoD agency or Service].

6. Duty Specialty or Occupational Code: [Be specific as possible].

7. Duration of Detail: [Provide a complete description].

APPENDIX F (CONTINUED)
DETAIL OF DOD PERSONNEL TO DUTY OUTSIDE OF DOD REQUEST TEMPLATE

8. Report Date: [Identify the proposed reporting date].

9. Required Security Clearance: [Identify the required clearance].

10. Description of Duties: [Provide a complete description].

11. Experience and Special Training: [Self-explanatory].

12. Reimbursable or Non-reimbursable: [Required; do not leave blank].

13. Justification of Non-Reimbursable Detail: [Provide a detailed justification with criteria for non-reimbursable. Details are provided in paragraphs 4.2.1. and 6.2.1 of reference (d)].

14. Benefits to the Department of Defense: [Provide specifics and detailed information, e.g., "fulfills important DoD required coordination for …", or critical impact on DoD coordination requirements within (agency)].

15. Other Requirements: [Provide information regarding other specific requirements not outlined above, e.g., "counterintelligence polygraph mandatory"].

APPENDIX G
ASSESSMENT STATEMENT TEMPLATE

ASSESSMENT STATEMENT

Recommendation: [Insert recommendation, such as: "Deputy Director authorize the Executive Assistant Director, Criminal Investigations Directorate, signature authority for the agreement because:"].

a. This is a [insert requirement, e.g. new agreement, updated agreement, three-year update] as required by NCIS-1, Chapter 51, and assignment responsibilities comply with NCIS mission contained in SECNAV Instruction 5430.107, Mission and Functions of the NCIS; SECNAV Instruction 5820.7C, Cooperation with Civilian Law Enforcement Officials, OPNAV Instruction 5530.14E, Navy Physical Security and Law Enforcement Program, and DoD Instruction 4000.19, Agreement Support. [Ensure all appropriate authorities are listed in this section, and delete any that are not applicable.]

b. The mission as stated in the MOU does not conflict with references contained in Chapter 51 relating to review requirements because of CI, CT, or HDI (does not impact intelligence, counterintelligence, and other sensitive activities sponsored or conducted by Governmental agencies). [Provide a justification statement for any affirmative response.]

c. Does not have the potential for public controversy or embarrassment, either domestically or overseas. [Provide a justification statement for any affirmative response.]

d. Does not have the potential to create unusual or significant risks to DON property and/or personnel. [Provide a justification statement for any affirmative response.]

e. Does not have the potential to cause adverse foreign military or diplomatic reactions or consequences. [Provide a justification statement for any affirmative response.]

f. Does not have the potential for negatively affecting DON relations with, or support to, other military departments or government agencies. [Provide a justification statement for any affirmative response.]

g. Does not contain DON-wide issues and DON-wide relations with, or support to, other military departments or government agencies. [Provide a justification statement for any affirmative response.]

h. Does not assign NCIS special agents outside of DoD. [Provide a justification statement for any affirmative response.]

APPENDIX H
OTHER USEFUL AGREEMENT TEMPLATE INFORMATION

The following template paragraphs may be inserted into agreements that require performance reviews or have time and attendance reporting requirements.

a. Performance Statement. NCIS is under a dual pay system. Intelligence analysts and directly related professional staff are paid and evaluated under the Defense Civilian Intelligence Personnel System (DCIPS). Special agents and the remainder of the professional staff are paid and evaluated under the General Schedule (GS) system. The NCIS employee's performance will be evaluated under the appropriate personnel system during the standard NCIS performance appraisal cycle of 1 October through 30 September.

(1) Performance objectives will be developed cooperatively by NCIS, the employee, and the employee's supervisor at the host activity within 30 days of reporting. DCIPS is a pay-for-performance system and accurate evaluation is essential. Thereafter, the employee's performance objectives will be reevaluated and reset annually and as needed to reflect the employee's actual performance requirements.

(2) The host activity supervisor will sign as immediate supervisor, and the NCIS supervisor will sign as the second-level supervisor. Copies of the proposed performance objectives will be provided to NCIS. Thirty days before scheduled review dates, NCIS will forward a reminder, guidelines, and suspense date to the host activity supervisor. The year-end appraisal will be forwarded to NCIS for the second-level supervisor's review and signature. Records of the host activity performance counseling will be retained by the host activity supervisor with copies forwarded to the NCIS supervisor with the rating of record.

Performance Evaluation Schedule		
Time period	**Evaluation level**	**Action required**
First 90 Days	Progress review	Immediate supervisor provides verbal evaluation to employee. No signatures required.
Mid-Point	Progress review	Written comments by the immediate supervisor are required. Employee and immediate supervisor sign cover sheet.
Annual	Rating of record	Written evaluation by the immediate supervisor is required. Employee and immediate supervisor sign cover sheet. Second-level supervisor's signature provided by NCIS. NCIS processes the evaluation according to GS or DCIPS guidelines.

b. Time and Attendance Report. NCIS will maintain the employee's time and attendance report. The NCIS employee is responsible for entering his or her time and attendance information into the SLDCADA system on a regular basis for certification by the NCIS supervisor. The NCIS employee will coordinate all leave requests with the host activity supervisor but will submit them through SLDCADA for approval by the NCIS supervisor.

APPENDIX I
AGREEMENT ADDENDUM TEMPLATE

MEMORANDUM OF UNDERSTANDING – ADDENDUM
BETWEEN
NAVAL CRIMINAL INVESTIGATIVE SERVICE
AND
NAME/TITLE OF OTHER AGENCY/UNIT/COMMAND

Subj: MEMORANDUM OF UNDERSTANDING – ADDENDUM FOR ORIGINALLY TITLED MOU

Ref: (a) Original MOU

1. Purpose. To amend reference (a) to include the following:

2. Background. Name/Title of other Agency/Unit/Command entered into reference (a) with NCIS on date of original agreement.

3. Period of Performance. This document will remain in effect for the duration of reference (a) or [state specific date].

4. Effective Date. This memorandum of agreement addendum becomes effective on the date signed by all parties listed in this agreement.

[Name of NCIS official] MM/DD/YYYY	[Name of official] MM/DD/YYYY
[Position/Title]	[Position/Title]
Naval Criminal Investigative Service	[Other party's organization]

NCIS-1, CHAPTER 53
NCIS PURCHASE CARD PROGRAM
EFFECTIVE DATE: AUGUST 2015

TABLE OF CONTENTS **PAGE**

53-1. Purpose. This chapter provides the policies and procedures for operating and managing the NCIS Government Purchase Card (GPC) Program. This chapter provides internal operating and management procedures for NCIS approving officials and cardholders. This guide does not supersede requirements set forth by higher authority.

a. This guidance should be used to assist management at all levels in properly discharging their responsibilities in the efficient management of the NCIS government purchase card program. These procedures are provided for exercising both technical and management controls to attain full and cost-effective use of funds.

b. References are listed in Appendix A, abbreviations and acronyms used throughout the chapter are listed in Appendix B, and common terms are provided in Appendix C. The procedures for purchase requests are provided as Appendix D, a list of items of common interest to purchase cardholders is provided as Appendix E, and the NCIS purchase card policy statement is provided as Appendix F.

53-2. Policy

a. As established in reference (a), the Government-wide commercial purchase card is the preferred method to purchase and pay for micro-purchases, which are procurements up to $3,000 using appropriated funds.

b. The DON obtains purchase card services from (b)(7)(E) The following guidance outlines operating procedures on the appropriate use of the purchase card by NCIS personnel.

(1) NCIS policy is to use the purchase card for all supplies and services at or below the micro-purchase threshold as either a procurement method or a method of payment ($3,000 for supplies, $2,500 for services, and $2,000 for construction).

(2) The purchase card must be used to purchase supplies and services for official U.S. Government business in accordance with DoD/DON regulations, instructions, policy letters/memorandums, and these procedures.

(3) The purchase card is to be used only for authorized U.S. Government purchases. Intentional use of the purchase card for other than official government business is considered an attempt to commit fraud against the U.S. Government and will result in immediate cancellation of the individual's purchase card and potential disciplinary action.

(4) In the absence of a specific statutory authority, purchasing items for the personal benefit of government employees, friends, and family, such as flowers and food, is not permitted and is considered an improper transaction. The use of the purchase card for personal purchases for any reason is strictly prohibited.

53-3. Cancellation. NCIS Purchase Card Internal Operating Procedures, 16 June 2014.

53-4. Chapter Sponsor. Acquisition and Logistics Department, Code 11B.

53-5. Responsibilities

a. Agency program coordinator (APC). The individual designated by the commanding officer or head of the activity who has overall responsibility for the management, administration, and day-to-day operations of the Purchase Card Program. The APC establishes and maintains their activity GPC program by appointing and documenting program participant authority in writing. The APC ensures program participants understand and perform their duties. The APC is the activity's point of contact with the issuing bank and monitors misuse of the card. The APC coordinates with approving officials, cardholders, and supervisors to ensure appropriate disciplinary action is taken.

b. Approving official (AO). The person responsible for reviewing and verifying the monthly purchase card statements of cardholders (CHs) under their purview. The approving official must verify that all purchases were necessary and for official government purposes in accordance with applicable directives. Unless otherwise specified, the AO will also be the "certifying official" for their CHs and must certify the monthly billing statement and forward it to the appropriate office for payment. AOs may not have more than seven CHs under their purview. An alternate AO must be identified, trained, and submitted to the APC to act on behalf of the primary AO in their absence. Only the AO or the designated alternate may certify monthly statements.

c. Cardholder (CH). The CH uses the GPC to acquire authorized supplies and services in accordance with their delegated authority. When making a purchase, the CH must comply with statutory, contractual, administrative, and locally applicable requirements. CHs ensure funds are available before making purchases and follow the specific limits according to their letter of designation (LOD). The CH must instruct merchants not to charge the GPC until after the supplies are shipped and request that the purchase be exempt from state sales tax. It is the CH's responsibility to review their monthly bank statement. The CH must reconcile their monthly

bank statement against their purchase log and other documentation, as they are accountable for erroneous payments resulting from the information they provide. The CH must keep their card secure; they should be aware of identity theft schemes and encrypt any email that contains account information or numbers. The CH must return the card to the APC upon leaving NCIS.

d. Supervisors. Supervisors are responsible for identifying program participants for GPC program duties and for implementing appropriate disciplinary action for negligence of duties, misuse, or abuse for program participants under their supervision. Supervisors will select trustworthy individuals to fill GPC roles and responsibilities and will remain actively involved in the performance of the GPC duties of the program participants they supervise.

53-6. Training

a. All candidates for purchase card accounts, including APCs, AOs, and CHs, must receive initial training and obtain a certificate to document training. The requirement to read NCIS-1, Chapter 53 will be documented by a signed statement acknowledging that the chapter has been read. Training requirements include:

(1) Online DON GPC training for their role.

(2) Defense Acquisition University course CLG0001.

(3) DoD ethics training (annual requirement).

(4) Training on NCIS Manual 1, Chapter 53.

(5) Certifying Official Training (certifying officials only).

b. Appointment of authority. After initial training, authority to perform primary program participant roles will be documented in writing by the APC before assuming a GPC program role and responsibility.

c. Refresher training. All GPC program personnel must complete activity internal operating procedures and purchase card refresher training every two years. Refresher training may be completed through one of the following methods:

(1) Regional training sponsored by the DON Consolidated Card Program Management Division.

(2) Defense Acquisition University course CLG0004.

(3) Online DON GPC training.

APPENDIX A
REFERENCES

(a) Federal Acquisition Regulation, Part 13–Simplified Acquisition Procedures, March 2005

(b) DON Consolidated Card Program Management Division website

(c) 18 U.S.C. §287, False, Fictitious or Fraudulent Claims, Edition 2012

(d) 10 U.S.C. §932, Art. 132, Frauds Against the United States, 3 January 2012

(e) 18 U.S.C. §1001, Statements or Entries Generally, Edition 2012

(f) NAVSUP Instruction 4200.99, Series, Department of the Navy (DON) Government-Wide Commercial Purchase Card Program Policy, 12 September 2012

(g) Federal Supply Schedule 75, General Services Administration, 5 December 2013

(h) 5 U.S.C. §4501-4507, Government Employees Incentive Awards Act, 3 January 2012

(i) SECNAV Instruction 7042.7K, Guidelines for Use of Official Representation Funds (ORF), 14 March 2006

(j) Memo, DoD Office of General Counsel, dtd 1 September 2005

APPENDIX B
ABBREVIATIONS AND ACRONYMS

APC	agency program coordinator
AO	approving official
CH	cardholder
DAPS	Defense Automated Printing Service
GPC	government purchase card
GSA	General Services Administration
HA	head of activity
LOD	letter of designation
MCC	merchant category code
PAT	program audit tool
PCAN	Purchase Card Administrative Notice
SCI	sensitive compartmented information

APPENDIX C
DEFINITIONS

1. Account limits. Use of the NCIS purchase card is subject to a single-purchase limit (usually $3,000), a monthly CH limit, and a monthly office limit.

2. Agency program coordinator (APC). The person designated by the Director, NCIS, to have overall responsibility for the management, administration, and day-to-day operations of the Purchase Card Program.

3. Approving official (AO). Local official responsible for reviewing and approving card billing statements to ensure each transaction was legal, proper, mission essential, and correct.

4. Billing cycle. The 30-day billing period. For the DON, the billing cycle begins on the 20th of the month and ends on the 19th of the next month.

5. Billing cycle office limit. Dollar amount assigned to the AO for the cumulative totals of the cardholders assigned.

6. Billing cycle purchase limit. The spending limit assigned to each cardholder for cumulative purchases and transactions within a given billing cycle.

7. Bulk funding. An advance reservation of funds where a commitment or obligation is recorded in aggregate rather than by individual transactions.

8. Cardholder (CH). The individual identified on the purchase card and the only user authorized to purchase U.S. Government supplies and services with the card. Purchase CHs are granted limited contracting authority by their head of activity (HA) or letter of designation (LOD).

9. Certifying officer. A DoD military member or civilian employee appointed in writing to certify a voucher for payment.

10. Contingency account. Contingency accounts are backup accounts and may be activated when the primary account holder is unavailable to perform purchasing actions. Contingency accounts will remain inactive until needed. The APC will set a credit limit of $1 on all CH accounts designated contingency accounts until the accounts are activated. Contingency cards are included in the span of control requirements.

11. Credit limit. The maximum dollar threshold assigned at the AO level limiting the amount an account may have outstanding at any one time.

12. Disputes. Instances in which the transactions on the CH statement conflict with entries in the log or retained receipts. This may include circumstances where the CH did not make the transaction, the amount of the transaction is incorrect, or the quality of the service is at issue.

13. Fraud. The use of the GPC to acquire supplies or services that are unauthorized and

APPENDIX C (CONTINUED)
DEFINITIONS

intended for personal use or gain. A purchase made for personal use or gain is internal fraud, and an unauthorized purchase made by someone other than the CH using a compromised card number or lost card is external fraud.

14. Head of activity (HA). The Director, NCIS, is the designated HA and may delegate responsibilities within the chain of command to a qualified individual other than the command APC. The HA or delegated official must complete DON HA training every two years.

15. Merchant category code (MCC). A four-digit code assigned to a participating purchase card vendor based on industry classification. The APC may limit CH transactions according to merchant type by blocking certain categories of vendors.

16. Monthly CH statement. The electronic summary of charges provided to the CH at the end of the billing cycle detailing all charges during that cycle.

17. Monthly billing statement. The official invoice for payment provided to the AO. The billing statement identifies all of the purchase card transactions of the CHs during a billing cycle.

18. Program audit tool (PAT). The DON data-mining tool, which requires the AO to review flagged transactions monthly. The AO must answer a series of questions for each flagged transaction. The answers will be reviewed and approved or rejected by the APC and DON Consolidated Card Program Management Division.

19. Purchase card. The credit-card-like account that enables properly authorized government personnel to buy and pay for mission requirements.

20. Purchase card log. A manual or automated log in which the CH documents mandatory government sources, screenings, and individual transactions using the purchase card. Entries must be supported by internal command documentation. Purchase card documentation should provide an audit trail supporting the decision to use the card and any required special approvals that were obtained.

21. Receipt. Documentation from the merchant showing the items purchased, unit price, total amount, date of the transaction, shipping and handling charges, and taxes (as applicable).

22. Reconciliation. The process by which the CH/AO reviews monthly statements, reconciles charges against vendor receipts and purchase card logs, and authorizes payment of charges on the monthly statement.

23. Recurring requirements. Recurring requirements for the same or similar supplies or services that exceed the micro-purchase threshold over a one-year period will be forwarded to the local contracting office to establish a blanket purchase agreement to meet future requirements.

APPENDIX C (CONTINUED)
DEFINITIONS

24. Services. As outlined in reference (a), services are firm fixed priced (including unpriced orders with an established ceiling) non-personal, commercially available requirements in which a contractor's time and effort is directly engaged to perform a task (e.g., repairs, maintenance, annual maintenance agreements).

25. Single-purchase limit. A dollar limit on each purchase assigned to each CH for a single transaction.

26. Split purchase/split requirements. Separating items to be purchased into multiple purchases to bypass the CH's purchase limit is prohibited. CHs may not break down requirements aggregating more than the simplified acquisition threshold or $3,000 micro-purchase threshold into several purchases less than the applicable threshold in order to simplify acquisition procedures or avoid exceeding the micro-purchase threshold.

27. Transaction type. The method by which an order is placed using the purchase card. Purchase card buys may be made in person, by phone, or through the Internet.

APPENDIX D
PURCHASE REQUESTS AND PROCEDURES

1. NCIS Purchase Request (PR)/Form 4238. Annotate all items, quantities, delivery information, unit prices, and attach supporting documentation on the NCIS PR/4238. The NCIS PR/4238 identifies justifications for purchase (mission essential/related) from the requester and the requirement to the CH. It also reflects purchase approval by the authorized personnel designated by the Finance department. NCIS CHs will ensure that sufficient funds are available and approved before making purchases.

a. CHs must screen all requirements from the mandatory sources of supply. For office, incidental janitorial, and sanitation supplies, CONUS CHs must purchase Ability One Supplies from DoD EMALL or local SERVMART. Small business and green products should be purchased to the maximum extent practical. Office furniture must be purchased from the Naval Supply Systems Command Fleet Logistics Center Norfolk suite of strategically sourced blanket purchase agreements.

b. Printing and duplication requirements and renting of duplication equipment must be purchased from DLA-Document Services.

c. Requirements for other supplies and services may be purchased from a local open-market source if the requirement can be met for a lower cost or faster delivery.

d. All IT requirements (hardware, software, cellphones, fax machines, pagers, scanners, copiers, etc.) must have Section 508 certifications and be routed to Code 15 for review and coordination, and to obtain an approved ITPR, in accordance with the DONCIO mandate. See reference (b), Purchase Card Administrative Notice (PCAN), 15 January 2013

(b)(7)(E)

e. Non-use of DON-directed sources. Occasionally, it may be impractical to purchase supplies and services from the DON-directed sources listed in Appendix D paragraphs 1a and 1b. In these circumstances, the AO must pre-approve the exception before the CH makes the purchase and justify why the DON-directed source was not used in the program audit tool.

f. CHs are authorized to use the purchase card for purchases made in person, over the phone, or through the Internet. All purchase card transactions must be documented on the CH's purchase card log.

g. CHs may ask their APC to request authorization of valid purchases that have been blocked by an MCC. This request must be emailed to the APC and validated by the AO.

2. Receipt and acceptance procedures. CHs are responsible for verifying receipt of all transactions. In an instance where the CH is billed but does not receive the supplies or services at the time of receipt of the official invoice, the CH must approve the statement in anticipation that confirmation of receipt will occur within the next billing cycle.

APPENDIX D (CONTINUED)
PURCHASE REQUESTS AND PROCEDURES

a. If the statement reflects an authorized purchase but the item has not been received, the CH must confirm with the vendor that the item has been shipped or is being delivered.

b. The CH must approve the statement charges and follow up to ensure the items are delivered within the next billing cycle. If the items are not received within the next billing cycle, the CH must dispute the charge through formal bank procedures.

c. If the billed items are not an authorized purchase, contact the vendor for a credit and initiate dispute procedures with Citibank. The CH must monitor the next statement to see the credit reflected. The CH must certify that the quantity and quality of the items furnished are in accordance with the agreement with the vendor. Review the vendor sales ticket for correct itemized charges. The CH must save all receipt documentation to properly reconcile the purchase card statement at the end of the billing cycle.

d. To protect the integrity of the procurement process and maintain internal controls, a three-way separation of function is preferred. If circumstances preclude an individual from performing a single function, a two-way separation of function, at a minimum, must occur for all purchase card transactions. For example, the same person may not initiate the requirement; award the purchase action; and receive, inspect, and accept the supplies or services. An individual other than the CH must record receipt/delivery of items delivered or services provided and submit a record of receipt/delivery to the CH. The record of receipt/delivery must include printed name, signature, date, telephone number, and office designator of person recording delivery, items received, and printed prices. **Contractors may not sign receipts or invoices.**

e. CHs and AOs must ensure that property valued at $5,000 and above is entered into the automated Defense Property Accountability System (DPAS), and pilferable items valued at $250 are properly identified.

3. Purchase Card Logs. All CHs must maintain either a manual or automated purchase log documenting individual transactions. The purchase card log and supporting documentation must provide an audit trail supporting the decision to use the card and any required special approvals that were obtained. The purchase log must contain the following (when applicable):

a. Required information to note:

(1) Purchase request number.
(2) Fiscal year.
(3) SDN from LOA block on Purchase Request.
(4) Date the item or service was ordered.
(5) The dollar amount of the purchase.
(6) Vendor Name
(7) A description of the item or service ordered.
(8) Date of receipt.

APPENDIX D (CONTINUED)
PURCHASE REQUESTS AND PROCEDURES

(9) Name of individual requesting the item or services.
(10) Name of individual accepting items or services.

b. Recommended information to note:

(1) Items that have been paid for but not yet received.
(2) Credit received.
(3) Dispute information.
(4) Required sources used/not used and justification.
(5) Remarks

4. Reconciling purchase card accounts. CHs must reconcile all transactions appearing on their electronic CitiDirect account for the billing cycle within three working days after the end of the cycle (normally the 19th of each month) by verifying the accuracy against CH records (NCIS PR/4238, receipts/invoices, etc.). The CH must review all information on the monthly statement, verifying any changes, credits, outstanding disputes, or refunds. The CH is responsible for purchase card transactions being proper and for notifying the AO of any information they have knowledge of that affects the propriety of certifying the monthly statement for payment. If transactions or credits are not included on the current statement, the CH must retain the applicable documentation until the transactions or credits appear and may be reconciled.

a. The CH must electronically approve/sign the (b)(7)(E) statement and electronically forward it to the AO for certification. The CH must forward all original purchase files (PR/4238s, receipts, invoices, logs) to the AO for review and retention. Each CH must ensure all required documentation is obtained and included in the forwarded purchase files. This includes NCIS Form PR/4238 or contracts, receipts/invoices with proper signatures, and approval/support documents. If the CH is unable to review their statement within the time allotted, the AO or alternate AO must review and approve the CH's monthly statement to complete the certification process within the eight-day grace period after the cycle closes.

b. If the monthly statement is not certified for payment by the end of the eighth day, both CH and AO accounts will be suspended immediately, and the appropriate DAD/SAC will be notified. Upon the CH's return, the CH will review the monthly statement and resolve any issues with the AO. Step-by-step CH procedures and tutorials for the (b)(7)(E) Card Management System are available on the DON purchase card website, see reference (b).

c. AOs are the certifying officials for the CHs assigned to their office account. The AO is responsible for ensuring all purchases made by the CHs within their cognizance were appropriate and that the charges are accurate. The AO must resolve all questionable purchases with the CH. In the event an unauthorized purchase is discovered, the AO must immediately notify the APC. The AO must sign or initial the invoice/receipt documents in the corner.

APPENDIX D (CONTINUED)
PURCHASE REQUESTS AND PROCEDURES

d. After review, the AO will electronically sign and certify the CH monthly statement in the (b)(7)(E) Card Management System. The AO must maintain the original supporting documentation for all purchases at their location so that it is accessible for review by the APC or higher authority. Monthly reconciliation packages retained by the AO must be originals and include (as appropriate) the following:

(1) PR/4238

(2) Copy of the monthly billing statement for each CH.

(3) Purchase card log for each CH, including entries for all listed transactions.

(4) Signed copy of the CH and AO certification page for each purchase card transaction.

(5) Copy of applicable contract, Defense Logistics Agency (DLA) Document Services DD Form 282 or training form SF-182.

(6) Invoice or vendor acknowledgement (must reflect item description, quantity purchased, unit price, shipping charges if applicable, and invoice total).

(7) Signed receipt for proof of delivery of services or supplies. These receipts must include printed name, title, signature and date, telephone number, and office code of person accepting delivery.

(8) Any other supporting documentation pertaining to the purchase (including IT approvals and Section 508 certifications). Step-by-step AO procedures and tutorials for the CitiDirect Card Management System are available on the DON purchase card website.

5. Reporting Requirements

a. APC monthly report. AOs must forward a copy of each CH's monthly purchase log with all transactions during the billing cycle to the APC no later than 10 days after the end of the billing cycle. The AOs must keep all original documentation (purchase requests, receipts, invoices, acceptance signatures, etc.) for all transactions filed by month at their location, accessible for review by the APC or higher authority. The APC must review transaction records on site visits to the AO's office. In addition, the APC will request additional documentation on randomly selected transactions on a monthly basis.

b. Program Audit Tool (PAT) review. AOs will electronically respond to all transaction review requests within 10 working days of the end of the transaction cycle. A complete review and response to all questions for any selected transaction is required. The APC may add transactions that appear to be questionable or need further explanation to the PAT review. This does not eliminate the requirement for the AO to review all transactions prior to certification for

APPENDIX D (CONTINUED)
PURCHASE REQUESTS AND PROCEDURES

appropriateness, accuracy, and complete documentation.

6. Retention of Records

a. Training records must be maintained by the AO for all CHs for three years beyond the time the employee is in the purchase card program. Records should include copies of all training certificates and any other written documentation on the CH's purchase card performance.

b. Transaction records must be maintained by the AO for six years and three months. AOs must maintain the official original transaction files (monthly reconciliation packages), including dispute transactions. Before disposing of financial documents, records retention officials must check with the comptroller for any supplemental retention guidance.

7. Merchant category codes (MCC) exemptions. Any purchase through a vendor that has an MCC code excluded by DON will cause an automatic declination by the banking system. A one-time exclusion may be requested to manually force the transaction. The CH must request the waiver by email to the APC via the AO.

8. Billing errors and disputes. CHs must immediately contact the vendor in an attempt to resolve any unauthorized charge or incorrectly charged amount. If the issue cannot be resolved with the vendor, the CH must file a formal dispute with the bank within 60 days of the charge. Examples of disputable charges include duplicate billing, non-receipt of merchandise, returned merchandise, canceled merchandise or services, invoice amount discrepancies, and transactions paid for by other means. Taxes and shipping charges are not disputable items through the bank and must be resolved with the vendor. The CH must notify the AO of disputed charges and handle all formally disputed transactions directly with the bank. See reference (b), PCAN 6, dated March 2013, for the distinction between "dispute procedures" and "fraudulent procedures."

9. CH restrictions. The CH and AO must comply with all local General Services Administration (GSA) and DoD/Navy regulations, and stay within the limits of their delegated authority letter.

10. Lost or stolen cards. If a purchase card is lost or stolen, notify (b)(7)(E) Customer Service immediately and the police (if applicable). If you are in CONUS, call (b)(7)(E) Customer Service at (b)(7)(E) If you are OCONUS, call (b)(7)(E) The CH also must notify (email is acceptable) the AO and APC on the next business day. Notification must include:

a. Card number.
b. CH's complete name.
c. Date, time, and location of the loss, if known.
d. If the card was stolen, the date the loss was reported to police and the report number.
e. Date and time (b)(7)(E) was notified.
f. Purchases made on the date the card was discovered missing.
g. Any other pertinent information.

APPENDIX D (CONTINUED)
PURCHASE REQUESTS AND PROCEDURES

11. Penalties for Unauthorized Use of the Purchase Card

a. A CH who makes unauthorized purchases or who uses the card in an inappropriate manner may be liable to NCIS for the total amount of the purchases made in connection with misuse, fraud, or negligence. Unauthorized use includes the use of the card by anyone other than the CH identified on the front of the purchase card. The GPC is for official government business only, and misuse, abuse, and payment delinquency will not be tolerated. Disciplinary actions will be determined on a case-by-case basis in conjunction with the immediate supervisor, Human Resources, and APC. Infractions may also be referred to the NCIS Office of Inspector General.

b. The CH may be held financially liable, as an accountable official to the government, for the amount of any payment certified and paid based on false or negligent information provided to the certifying officer. In accordance with reference (c), misuse may result in a fine of not more than $10,000 or imprisonment for not more than 5 years, or both. Military members who misuse the purchase card are subject to court-martial, in accordance with reference (d).

c. Making false statements on purchase card records may be cause for removing an employee from Federal service. Punishment for making false statements may include fines, imprisonment, or both, as stated reference (d).

d. If a card that was reported lost or stolen is later found, the CH must destroy the card in front of a witness and provide written notification to both the APC and AO.

12. Transfer or Separation of a CH or AO

a. The CH and AO must ensure, to the maximum extent possible, that the CH's account is inactive for at least 30 days prior to the projected dated of transfer, retirement, or termination. Both the CH and AO are responsible for ensuring all charges have been billed against the account, all credits have been received, disputes have been resolved, and all requirements have been received and accepted by the government. The AO must notify the APC in writing (email is acceptable) that there are no outstanding transactions and request closure of the account. Notification should include a statement that the card was destroyed and witnessed. The account must be closed by the employee's last workday.

b. Activities must ensure there is no lapse between AOs. A new AO must be identified, trained, and appointed before the outgoing AO departs. If a new AO is not appointed prior to the outgoing AO's departure, all CHs under that account will be suspended until the new AO is appointed. When a CH leaves the activity, all files documenting GPC transactions must be turned in to the current AO for retention.

13. Inactive Accounts. The APC shall ensure that CH accounts that have not been used in the previous six months or that were used less than three times during the preceding six-month period are closed unless the supervisor submits an acceptable justification to the APC for

APPENDIX D (CONTINUED)
PURCHASE REQUESTS AND PROCEDURES

keeping them open. Under some circumstances it may be appropriate to hold inactive accounts open. These include, but are not limited to, contingencies, deployed-status accounts, or cases when an employee is on extended sick leave or experiences a temporary disability.

14. Government purchase card as a "method of payment." The card will be used as a method of payment for the following (if authorized in CH's letter of delegation):

a. Request, authorization, agreement, certification of training and reimbursement (SF-182).

(1) The SF-182 may not exceed $25,000. This form is authorized for costs associated with individual and group attendance.

(2) The training must be an off-the-shelf event, conference, or course available to the general public and priced the same for all attendees (e.g., price per student, course, program, service or training space).

(3) CH must state payment is to be made by Government Purchase Card in block 27.

(4) In most cases, the purchase card will not be accepted if training is to be provided by a State, Federal, or another DoD agency.

b. DoD Printing Requisition/Order (DD Form 282) valued at $24,999 and below.

(1) All printing or duplication requirements must be forwarded to the Defense Logistics Agency (DLA) Document services, which is the authorized agency for DON printing.

(2) CHs must ensure that the appropriation block of DD Form 282 reflects that payment will be made with the purchase card. The CH's name and telephone number should be stated in the special instruction/remarks block. Do not include the card number. When DLA Document Services completes the printing request, the CH will be called to furnish the card number.

c. Purchase orders (SF-1449/DD 1155) valued up to $150,000 or commercial items up to $6.5 million.

d. Delivery orders against Federal Supply Schedules valued up to $9,999,900.

e. Basic Ordering Agreements and orders under Indefinite Delivery Type Contracts valued up to $9,999,900.

f. Oral orders against Letters of Agreement valued between $2,500 and $25,000 for procurement of supplies only.

APPENDIX D (CONTINUED)
PURCHASE REQUESTS AND PROCEDURES

15. Vendor rotation. CHs are required to rotate requirements among qualified suppliers to the maximum extent practical.

16. Cash refunds. Under no circumstance may a CH accept a cash refund for non-receipt, returned, or damaged items purchased with a GPC. CHs must accept credit to the account.

17. Gift checks, rebates, or incentives**.** Under no circumstance may a CH retain gift checks, vendor rebates, or other purchase incentives that could be converted to personal use. If received, they must be turned over to the U.S. Treasury. Contact the NCIS Comptroller for guidance.

18. Card security. CHs are responsible for the security of their purchase cards. Purchase cards should be safeguarded in the same manner as cash. The named CH is the only official government representative authorized to use that purchase card.

19. DON purchase card website. Additional guidance and all forms and guides for the GPC program are available at reference (b). This site includes all guidance from the Consolidated Card Program Management Division (CCPMD) and Citibank. It is highly recommended that CHs and AOs register at the site to receive updates. This chapter provides the CH and AO basic purchase card guidelines; however, these procedures are not all-inclusive, and each purchase card participant is responsible for remaining current on all instructions and notices pertaining to the purchase card program. See (b)(7)(E) for more information.

APPENDIX E
COMMON INTEREST ITEMS

The following is provided as general guidance on topics that people frequently have questions about. For more specific guidance, contact the APC in Code 11. Note: CHs may make purchases from merchants that use a third-party payment vendor, such as PayPal, only if no other merchant is available. Also, individuals may not benefit personally from refunds or rebate checks. Checks must be made out to the U.S. Treasury, DON, or NCIS, and forwarded to the Comptroller.

1. Advance payments

a. Advance purchase card payments are prohibited except for requirements, such as subscriptions for publications (*Navy Times*, *Federal Contracts Reporter*, etc.) and post office box rentals. Subscriptions must be held to a minimum consistent with operational requirements. Each PR/4238 for subscriptions must contain certification by the DAD/SAC that the periodical is necessary for operational purposes.

b. Advance payment of tuition and other expenses is authorized if the training facility renders or refuses to render a billing, or if advance payment is indicated in SF-182 section "g."

2. Advertising. Advertising contract actions are not authorized unless specific approvals have been obtained.

3. Allowable services. Firm fixed price repair orders, including automobile repairs (if the Fleet card is not accepted), are allowable charges. Firm fixed-price services must be performed within 30 days from the date the order is placed. Other examples of allowable services include Internet access, rental or lease of cellular and pager services, hardware and software maintenance, copier rentals, and credit report services. The annual amount cannot exceed $2,500. Services are limited to 12 consecutive months except for subscriptions. (Internet access and access to online services are not considered subscriptions.) See Appendix D, paragraph 1d.

4. Ammunition and weapons. CHs are not authorized to buy ammunition or weapons. Ammunition and weapons are obtained by NCISHQ from Naval Sea Systems Command and are shipped directly to each field office bunker for distribution to assigned special agents.

5. Asbestos and asbestos-containing materials. CHs are not authorized to purchase asbestos or asbestos-containing materials.

6. Base Exchange. CHs are authorized to buy from Non-appropriated Fund Instrumentalities/ Morale, Welfare, Recreation and exchanges. Prior to ordering, the CH must screen the requirement from the mandatory government services of supply (DoD EMALL or SERVMART) and Environmentally Preferred Products. Supplies must be in stock when the order is placed, and the CH may not special order a requirement not regularly provided by the exchange.

7. Bottled water. Appropriated funds should not be used to purchase or rent water coolers and bottled water service unless a qualified medical/health professional has officially identified the

APPENDIX E (CONTINUED)
COMMON INTEREST ITEMS

local water as non-potable. A copy of the authorization letter must be attached to each statement reflecting a charge for bottled water service.

8. Buildings and/or land, rental or lease of. CHs are prohibited from entering into long-term rentals or leases for buildings or land.

9. Business cards. Members of the senior executive service (SES) may authorize the printing of business cards, limited to using existing software and agency-purchased stock or cards procured from Ability One if the cost of is equivalent or less than producing the cards on a personal computer. Business cards obtained under this authority will be used for those positions that require business cards in the performance of their official duties. CHs are not authorized to purchase printed business or calling cards.

10. Cash advances. CHs are prohibited from using the purchase card to obtain cash advances.

11. Christmas and other seasonal decorations. Seasonal decorations may be acquired using the purchase card, provided local customs and traditions are observed. Purchase CHs are not authorized to buy Christmas cards.

12. Coffee pots and coffee. The purchase of common-area kitchen equipment, such as coffee pots, coffee, refrigerators, microwaves, and other related items, for the purpose of supporting military and civilian employees in the workplace is authorized if the primary benefit is collateral, not individual.

13. Conference room rentals. CHs are authorized to obtain short-term conference room rentals.

14. Conference, registration, or training fees. Use of the government purchase card for conference/registration fees is allowable under the following basic guideline. A conference fee that includes meals, an event that has been authorized for the employee to attend, is a proper use of appropriated dollars. If meals are included in the conference fee, the traveler must indicate when filing for travel expenses that meals were provided so that the government does not pay twice, but instead, reimburses the traveler for legitimate charges only (reduces per diem). A government employee may attend a non-government-sponsored meeting at government expense and have the conference fee paid if:

a. It is part of an authorized training program, or
b. It is related to agency functions or management.

15. Construction. Purchase CHs are authorized to purchase facilities improvement services worth up to $2,000 and facilities supplies up to $2,500.

a. Improvement services examples. Painting and janitorial. CHs may not purchase pesticides, including pest control services.

APPENDIX E (CONTINUED)
COMMON INTEREST ITEMS

b. Facility improvements examples. Erecting walls, repairing walls, making doorways, installing electrical outlets, and making or repairing holes in the wall.

16. Commercial vehicles. CHs may not use the purchase card to buy commercial vehicles.

17. Rental/lease of commercial or GSA vehicles (without drivers). CHs are not authorized to use purchase cards to rent or lease commercial or GSA vehicles unless used as a "method of payment" on an existing contract.

18. Employee identification tags. The Office of Military Services may authorize purchase of military identification tags if it is determined that they are necessary and support mission requirements.

19. FedEx, UPS, and similar shipping methods. The purchase card may be used for the purchase/payment of FedEx or similar services for administrative shipments. The CH must establish an account first, however.

20. Fuel, oil, services, maintenance, or repairs. Purchase CHs are not authorized to purchase fuel, oil, services, maintenance, or repairs of Interagency Fleet Management System (IFMS) and GSA Fleet Management Programs (i.e., repair of GSA-leased vehicles). Exception: CHs may use the card to procure gasoline or oil for DON vessels if a Fleet Card is not available and the requirement falls within the following criteria:

a. Vehicle is DON owned.
b. CONUS/Alaska locations—less than 10,000 gallons annually.
c. OCONUS/Hawaii—less than 20,000 gallons annually.

21. Hazardous material (hazmat). CHs are authorized to buy commonly used hazardous materials or products that are customarily sold to the general public to be used for non-governmental purposes (commercial products), and which are in the same size and packaging found commercially. Examples include those products required on a routine basis to meet daily operational needs, such as toner cartridges, ink-jet cartridges, batteries, copier supplies, lubricants, detergents, and fax film. Safety data sheets are required for anything that contains hazardous materials. CHs must be in compliance with local base policies and procedures for this type of purchase.

22. Household goods transportation services. The use of the purchase card to procure household goods transportation services is prohibited.

23. Incidental janitorial and sanitation supplies. All incidental janitorial and sanitation equipment and supplies must be purchased through DoD EMALL or at local base supply stores. See reference (b), PCAN 3 December 2012 at

(b)(7)(E)

APPENDIX E (CONTINUED)
COMMON INTEREST ITEMS

24. Information Technology (IT) Resources

a. IT/ADP certification is required from Code 15 prior to purchase. Do not process any IT procurements without approval from Code 15. See reference (b). Contact Code 15 for written authority prior to purchasing any handheld digital devices. Documentation must be attached to the PR/4238. See Appendix D, paragraph 1d.

b. IT requirements examples: All computer-related hardware (computers, printers, modems, laptops, routers, servers, and networks), fax machines, commercial software, cellular phones, pagers, and any equipment containing embedded microchips. See Appendix D, paragraph 1d.

25. Lodging and meals. Purchase CHs are prohibited from using purchase cards for payment of lodging and meals for employees, whether or not they are on temporary duty. However, certain reserve activities are authorized to buy meals for Naval reservists during drill activities.

26. Luggage. The purchase of luggage for employees or Service members to carry personal belongings while on travel orders is generally not authorized. However, sea bags issued to Service members and briefcases, etc., furnished for the express purpose of carrying official documents associated with the duties of the Service member or employee is allowed.

27. Medical and dental care from civilian non-Federal sources

a. The purchase card may be used to pay for annual physicals (not routine health care) for special agents because they are a condition of employment. However, whenever possible, the physical must be performed at the nearest military medical facility.

b. When a military medical facility is used, the office manager must contact the NCIS Comptroller for guidance. Payment will be made via a reimbursable document accomplished by either a NAVCOMPT Form 2275 or Military Interdepartmental Purchase Request. The card may be used for medical exams, lab work for rape cases, etc.

28. Membership dues

a. The purchase of club, association, organization, and other related memberships—except those memberships that solely benefit the agency or activity—are prohibited.

b. Navy exception: The use of appropriated funds for membership dues of an activity or agency is permissible if the membership contributes to the fulfillment of the mission of the activity or agency. The membership must be in the name of the activity or agency, not an individual's name. The membership cannot be for a position of management or control of the professional association.

APPENDIX E (CONTINUED)
COMMON INTEREST ITEMS

c. NCIS exception. NCISHQ has authorized payment for memberships by official position in the International Association of Chiefs of Police. It is recognized that many other professional law enforcement associations exist at the national level, possibly warranting membership by NCIS. Such memberships must comply with Navy guidance. Payment must be justified in writing and favorably endorsed by the SAC/DAD, as appropriate.

29. Office decorations. Purchase CHs are authorized to buy artificial or real decorative plants, pictures, posters, etc., for general office use when a need for such items is determined by an agency official and decorations are permanent additions to office décor and result in improved productivity and morale.

30. Office Supplies

a. All office supplies must be purchased through DoD EMALL or at local base supply stores. Reference (f) outlines the policy. Reference (g) defines office supplies as commercially available off-the-shelf office items. Examples include binders, clips and fasteners, staplers, pencils, pens, paper, printer and toner cartridges, calendars, pads, notebooks, desk accessories, filing supplies, Post-it notes, scissors, tape, waste containers, and CDs.

b. OCONUS activities are encouraged to use DoD EMALL to the fullest extent possible and prior to using any other online shopping tools. The waiver does not preclude the requirement to screen for and purchase from mandatory sources.

31. Personal services. CHs may not contract for personal services using the purchase card.

32. Pesticides. CHs are not authorized to contract for the purchase of pesticides unless prior approvals are obtained from the pest management consultant at the appropriate Naval Facilities Engineering Command.

33. Plaques, paperweights, and other give-away mementos

a. The use of appropriated funds to buy give-away items, such as plaques, cuff links, pictures/posters, hats, T-shirts, license plate covers, bracelets, clocks, ashtrays, paperweights, cigarette lighters, novelty trash cans, key chains, and similar items, as gifts for retirements, transfers, etc., is generally prohibited. An agency may not use appropriated funds to purchase gifts or other personal items unless it has specific statutory authority to do so (as in the case of employee awards in reference (h) or can demonstrate a direct link between the items and the accomplishment of an authorized agency purpose or mission (as opposed to publicity for the mission's existence).

b. Give-away items, such as mementos, may be purchased in support of employee recognition programs if they are acquired in accordance with agency policy. The mementos must be command mementos, such as plaques, and not personal items. Such mementos may not

APPENDIX E (CONTINUED)
COMMON INTEREST ITEMS

be presented to DoD personnel. When items are presented within the authority of reference (i), a complete record must be maintained in the CH purchase or transaction files to include the name(s) of the recipient(s) and the reason for the presentation.

34. Pre-paid phone cards. CHs may buy pre-paid phone cards as long as they are secured and monitored to ensure they are for official use only.

35. Printing, copying, duplication. Purchase CHs are prohibited from buying printing or duplication services from agencies other than Defense Logistics Agency (DLA) Document Services. All printing requests must be submitted to DLA on a DD Form 282. If DLA is unable to complete the printing, procuring printing from other sources, such as a commercial printing company, is permitted. NCIS purchase CHs are authorized to use the purchase card as a method of payment for DD Form 282. To purchase printing/duplication services outside of DLA, the CH must have prior DLA written approval. Approval must be attached to the funding document.

36. Radio frequency and wireless devices

a. Purchase CHs are not authorized to procure radio frequency or wireless devices unless prior approval from the Installation Spectrum Management Office is obtained. Radio frequency and wireless devices include fixed and mobile radio transmitters, radars, microwave radios, computer wireless technology, and commercial off the shelf radio frequency wireless technology. See Appendix D, paragraph 1d.

b. Provided approval was obtained for the original purchase, purchasing exact replacement parts for existing systems does not require approval.

37. Recruitment booths. College recruitment booths are not considered advertising and therefore are an allowable expense that does not require special approval. However, recruitment advertising in newspapers, magazines, television, and radio and online requires special approval external to NCIS prior to purchase.

38. Refreshments

a. For specific guidance, see reference (j).

b. Food is a personal expense for which appropriated funds are not available, absent legal authority. The following is a list of recognized exceptions—some overlap—to the general rule in the context of conferences, meetings, and events.

(1) Award ceremonies. Food may be purchased only if:

(a) The award recipients are either Federal employees or military members.

APPENDIX E (CONTINUED)
COMMON ITEMS OF INTEREST

(b) The award recipients are publicly recognized.

(c) The authorized agency official has determined that food materially advances the recognition of the recipient.

(2) Cultural awareness ceremonies. Food may be purchased only if:

(a) It is part of a formal program intended to advance EEO objectives and make the audience aware of the cultural or ethnic history being celebrated.

(b) It is indicative of the culture and is offered as part of the larger program to serve an educational function.

(c) The portions and selection do not constitute a meal.

(3) Training

(a) Appropriated funds may be used to cover food costs that constitute a non-severable portion of the registration or attendance fee for a training program.

(b) Food costs are considered non-severable if they are billed as part of the overall costs of the conference, and the conference costs cannot be reduced by foregoing the food or by breaking out the food costs as a separate optional item.

(c) The cost of food provided at a training program conducted by the government is presumed to be severable because the government is responsible for arranging the program.

(d) If food costs are a severable part of the registration fee, appropriated funds are available for such costs only where necessary for the employee to obtain the full benefit of the training. For example, where essential training is conducted during a luncheon session, food may be provided at government expense. Simply labeling a session as a "training event" is not sufficient; instead, the event must be a substantive program designed to improve trainee and agency performance.

39. Reprographic equipment

a. The purchase, lease, rental, trial, replacement or change in rental or lease plan of reprographic equipment is not authorized unless the requestor has complied with the requirements of the Navy Reprographic Equipment Program. (Examples of reprographic equipment include copiers, diazo process equipment, laser printers, and duplicating equipment.) See Appendix D, paragraph 1d.

APPENDIX E (CONTINUED)
COMMON INTEREST ITEMS

b. Purchase CHs may purchase, lease, rent, trial, replace, or change copiers that make fewer than 71 copies a minute and laser printers that produce fewer than 20 copies a minute. If existing

equipment meets those standards, CHs must obtain written approval from their supporting DLA office to obtain the desired equipment.

40. Retirement seminars. Use of the GPC is allowed for fees associated with the enrollment of Government personnel to attend government- or non-government-sponsored retirement seminars.

41. Safety/Specialty Clothing

a. Safety clothing, footwear, or ergonomic equipment. Requests for any type of safety clothing, footwear, ergonomic equipment (personal protective equipment (PPE) under OSHA and its implementing regulations) requires written approval from the NCIS Safety Officer.

b. Special clothing and equipment. Appropriations are available for the purchase and maintenance of special clothing and equipment for the protection of personnel in the performance of assigned tasks. The item must remain property of the government and satisfy the following requirements to be authorized and procured with appropriated funding:

(1) The item must be "special" and not part of the ordinary and usual furnishings an employee may reasonably be expected to provide for themselves.

(2) The item must be for the benefit of the government, that is, essential to the safe and successful accomplishment of the work and not solely for the convenience of the employee.

(3) The item could be destroyed due to the nature of the work (e.g., cleaning an oil tank).

(4) The employee is engaged in hazardous duty.

(5) The clothing meets the government's "minimum need" and the government assumes responsibility for issuing, tracking, cleaning, storage, and repair of the clothing.

42. Sensitive compartmented information (SCI). Contact the NCIS Special Security Officer (Code 11A) for guidance on SCI, JWICS, and items that are classified or sensitive in nature.

43. Service Requirements

a. CHs may purchase services up to 12 months per transaction; however, the annual amount may not exceed $2,500. Examples of service requirements include copier lease/rental, cellphone service, Internet access, online computer services, hardware/software maintenance, and credit bureau services. Automobile repairs may be purchased if the vendor will not accept the Fleet card. (Internet and online services access are not subscriptions.) See Appendix D, paragraph 1d.

APPENDIX E (CONTINUED)
COMMON INTEREST ITEMS

b. CHs may not purchase FTS 2000, DSN, or base telephone systems.

44. Towing/vehicle repair. CHs may buy vehicle-towing services if the Fleet card is not accepted. CHs must note on the PR/4238 why the Fleet card was not used; examples include:

a. No local auto service repair centers that accept the Fleet Card were available.

b. The vehicle is under maintenance warranty; warranty work must be performed by a dealership that does not accept the Fleet card. The purchase card may not be used to repair/tow Interagency Fleet Management System (IFMS) and GSA Fleet Management Programs vehicles (GSA-leased vehicles).

45. Training

a. The SF-182 is authorized for training costs associated with individual and group attendance under the following conditions: The training is an off-the-shelf event, conference, or instructional service available to the general public and priced the same for everyone (e.g., price per student, course, program, service and/or training space). Purchase CHs may use the card as a method of payment for training requirements using the SF-182 valued at $25,000 and below.

b. Training requests must be submitted to Code 10B at least 21 days before the training starts. Email is the preferred notification for training requests.

c. Annotate in Section 3 of the training request if your code/field office is paying for the training and any associated travel. If your code/field office is funding the training, provide a point of contact, including a commercial phone number.

d. Training must be pre-approved before obligations or commitments are formalized with a training provider. Training is authorized and paid for via the SF-182 (Request, Authorization, Agreement, Certification of Training and Reimbursement). Payment is generally made using the GPC. The SF-182 is the only method for payment of training costing less than $25,000.

46. Travel or travel-related expenses

a. The purchase card may not be used to pay for official travel or travel-related expenses such as transportation, lodging, or meals.

b. Conference fees that include lodging and meals, conference rooms, meeting spaces, and local transportation (such as Metro fares, EZ Pass, and subway tokens) are allowed.

47. Organization items/equipment. Organizational or personal protective clothing that remains the property of the organization may be purchased with the GPC.

APPENDIX F
NCIS PURCHASE CARD POLICY STATEMENT

The Approving Official or Cardholder (as Accountable Officials) certifies that:

1) I have read the NCIS-1, Chapter 53, Purchase Card Program.

2) I will ensure that funding is available and approved by the Comptroller via a purchase request (PR) or NCIS Form 4238 prior to any purchases with the government purchase card.

3) I understand I may be financially liable for purchases made without prior approval.

_____

Print Name

_____

Signature and Date

NCIS-1, CHAPTER 56
NCIS INSIDER THREAT PROGRAM
EFFECTIVE DATE: OCTOBER 2014

TABLE OF CONTENTS **PAGE**

56-1. Purpose. This chapter establishes the NCIS Insider Threat Program (ITP), assigns program responsibilities, and provides policy to guide program implementation. The ITP is designed to protect NCIS from insider threats, defined as the actions of persons with authorized access who use that access, wittingly or unwittingly, to harm national security interests or national security through unauthorized disclosure, data modification, espionage, terrorism, or kinetic actions resulting in the loss or degradation of resources or capabilities. In this context the term, kinetic actions, includes threats and acts of workplace violence. This chapter pertains only to the internal NCIS ITP. NCIS roles and responsibilities in support of the overarching DON Insider Threat Program are a separate matter. References are provided in Appendix A, and acronyms and abbreviations used in the chapter are listed in Appendix B.

56-2. Policy. The ITP will operate within the context of the laws and regulations governing individual rights and privacy. It serves to protect all employees while respecting the civil liberties, rights, and privacy of each employee. This policy applies to all employees as defined in Appendix C. Specific roles and responsibilities are outlined in Appendix D. For more information, see the NCIS Internal Insider Threat Program[1] page on Lighthouse.

a. NCIS intends to maintain a professional and harmonious work environment within which personnel issues of concern and counterproductive behaviors are detected and mitigated before they pose an insider threat, and where malicious insiders face a daunting risk of detection.

b. NCIS strives to minimize the incidence of insider threats by carefully vetting prospective employees for suitability, trustworthiness, and reliability; by providing the training and development necessary for employee success; by carefully assessing probationary employees for continued service to NCIS; through effective employee supervision; by establishing realistic

[1] Available at:

(b)(7)(E)

performance plans and seeing them through to completion; by holding all employees accountable for their performance and behavior; and by seeking to assist employees with the resolution of work-related issues and personal problems in the early stages. The ITP can back stop, but not replace, these fundamental individual and organizational responsibilities.

c. ITP reporting requirements are listed in Appendix E. Security reporting requirements are listed in Appendix F.

56-3. Cancellation. None.

56-4. Chapter Sponsor. Security Manager (Code 11A), in the role of designated Insider Threat Senior Official.

56-5. Background. NCIS must protect the safety of its personnel and resources from insider threats, those who—out of anger, frustration, greed, disaffection, alienation, or a lapse of judgment, ethics, integrity, or training—pose a threat to NCIS, the DON, or the DoD. NCIS personnel routinely accesses highly classified and sensitive compartmented information, and firearms are standard equipment for special agents and certain other employees. Although the workforce is highly professional, carefully vetted, and continuously evaluated in accordance with the regulations governing access to classified information, and armed personnel are regularly trained in the authorized and safe usage of firearms, these measures do not eliminate the risk of insider threats. In accordance with references (a) and (b), an ITP is required to identify, mitigate, and manage the remaining risk.

56-6. Authorities

a. The authority to investigate any information indicating that retaining any employee may be inconsistent with national security interests is contained in reference (c).

b. Reference (d) directs structural reforms to improve the security of classified networks and the responsible sharing and safeguarding of classified information. The reference:

(1) Establishes the requirement and assigns responsibilities for insider threat programs.

(2) Establishes authorities and relationships specific to the implementation and oversight of insider threat programs.

(3) Directs the integration of counterintelligence, information assurance, antiterrorism, force protection, security/law enforcement, and human resources information for the purpose of insider threat detection and prevention.

(4) Directs material support from and coordination with legal and civil liberties entities.

56-7. Organizational structure. The ITP's organizational structure emulates the template in reference (e). The National Insider Threat Task Force (NITTF) template will be adapted as necessary to accommodate NCIS' mission, organizational, and resourcing requirements.

Pages 1212 through 1227 redacted for the following reasons:
- -
(b)(7)(E)

NCIS 1, CHAPTER 58
PEER SUPPORT PROGRAM
EFFECTIVE DATE: AUGUST 2015

TABLE OF CONTENTS **PAGE**

References:
(a) NCIS 1, Chapter 56, Insider Threat Program, October 2014
(b) DoD Directive 5240.06, Counterintelligence Awareness and Reporting (CIAR), 17 May 2011
(c) NCIS 3, Chapter 41, Major Incidence Response, May 2015
(d) NCIS 1, Chapter 50, Casualty Assistance Program, June 14, 2011
(e) DON Civilian Employee Assistance Program website
(f) 5 CFR Part 792, Federal Employees' Health and Counseling Programs

58-1. Purpose. This chapter establishes and provides guidance for the Peer Support Program (PSP), including the program's structure, roles and responsibilities, and the means by which support is provided.

58-2. Policy. The Peer Support Program provides all NCIS employees the opportunity to receive emotional and tangible peer support through times of personal or professional crisis and to help anticipate and address potential difficulties.

a. Peer support programs help people cope with a wide range of personal and work-related issues. The rationale for such a program is that individuals who share common conditions or experiences can cope more effectively by discussing their experiences, sharing practical information, and offering moral support to one another.

b. The PSP will maximize existing agency resources by providing employees with additional options and tools for dealing with personal problems. The support program is staffed by peer support responders under the supervision of a licensed clinical psychologist, an agency program coordinator, and an assistant program coordinator. Peer support responders are full-time NCIS employees who have been specially trained to assist fellow employees by providing information, guidance, and advice. Peer support responders voluntarily assist program participants in addition to their regular work assignments. They may conduct peer support activities, provided that doing so does not interfere with their regular work assignments, violate agency policies or procedures, or otherwise disrupt operations. Peer support responders do not provide professional services, such as diagnosis or treatment of mental disorders, psychological assessment, testing, counseling, or any other activity that might constitute the practice of psychotherapy.

c. Although the PSP may recommend that participants seek outside resources, recommendations do not constitute official sanction or endorsement of a particular provider by the PSP or NCIS.

58-3. Cancellation. None**.**

58-4. Chapter sponsor. Office of the Ombudsman.

58-5. Definitions

a. Agency program coordinator. Oversees the PSP's operations by appointment of the Director and acts as the formal liaison between peer support responders and the clinical psychologist.

b. Assistant program coordinator. Lead peer support responder who assists in overseeing PSP operations.

c. Peer support responders. Full-time NCIS employees selected and trained to provide a first line of assistance and basic crisis intervention to fellow employees. Peer support responders are volunteers who assist program participants during times of personal and professional crisis and are trained to recognize situations that may require additional resources. Peer support responders may be special agents or professional staff. Peer support is a collateral duty. Peer support responders may engage directly with the clinical psychologist.

d. Program participants. Employees who have contact with peer support responders in their role as peer supporters.

58-6. Organizational structure. The PSP maintains policy, program participant statistics, and meeting agendas, as well as conducts continuing education and program participant review with the clinical psychologist. The PSP organizational structure is as follows:

a. Agency program coordinator

(1) Maintains the integrity and accountability of the PSP.

(2) Coordinates the formulation and administration of PSP policies, procedures, guidelines, and directives.

(3) Ensures adequate administrative support for the program.

(4) Ensures adequate funding for the program.

(5) Coordinates the resolution of program-related problems and considers complaints and grievances related to peer support responders and program function.

(6) Coordinates the selection and training of peer support responders.

(7) Promotes the PSP throughout the agency.

(8) Serves as a liaison to the clinical psychologist.

(9) Facilitates peer support responder meetings.

b. Assistant program coordinator

(1) Assists in formulating and administering PSP policies, procedures, guidelines, and directives.

(2) Serves as lead peer support responder.

(3) Coordinates program funding.

(4) Assists in resolving program-related problems and considers complaints and grievances related to peer support responders and program functioning.

(5) Maintains statistics and other documentation (less personally identifiable information) of program activities.

(6) Assists in selecting and training peer support responders.

(7) Coordinates training.

(8) Assists in promoting the PSP within the agency.

(9) Collects data from contact sheets to gauge use and effectiveness of program.

c. Clinical psychologist

(1) Provides annual training.

(2) Consults on the program and with peer support responders.

(3) Provides consultation during a critical incident.

d. Peer support responder

(1) Ensures program participants understand that while the PSP greatly emphasizes confidentiality, there are certain specific circumstances in which the peer support responder is required to directly report information without first seeking consent.

(2) Avoids actual or perceived conflicts of interest.

(3) Ensures program participants understand the role and limitations of the peer support responder.

(4) Conducts themselves in a neutral, non-partisan manner.

(5) Appropriately maintains confidentiality of personal information and/or information revealed by program participants and reports such information only when required.

(6) Avoids giving legal advice.

(7) Avoids giving independent advice and/or opining about management decisions and/or personnel actions.

(8) Avoids discussing personal and/or Privacy Act-protected information regarding other employees' personal or professional situations in a manner that may identify the individual.

(9) Maintains contact sheets and provides metrics to the agency program coordinator.

(10) Avoids taking notes during sessions with program participants.

58-7. PSR Selection and Program Requirements

a. Eligibility. All full-time employees who meet the following guidelines are eligible:

(1) Completed any initial trial period.

(2) Are not on a performance improvement plan.

(3) Do not have a current letter of reprimand or letter of requirement.

(4) Are in good standings within the agency (as verified through various directorates).

(5) Have successfully completed the application process and training.

b. Selection and de-selection. Applications for peer support responders will be solicited as program needs dictate. The selection process involves an assessment board consisting of the clinical psychologist, agency program coordinator, and assistant program coordinator.

(1) The assessment board may consider characteristics and traits such as the applicants' reputation, credibility, and integrity within the agency and among their peers; social skills; ability to empathize; education and training; job experience; use of this or a similar programs; motivation; sincerity; ability to complete training; and adherence to program policy.

(2) Selected peer support responders must sign a memorandum of understanding/ confidentiality statement and successfully complete all required training.

(3) Due to the sensitive nature of peer support responder work, peer supporters may be non-selected or de-selected at any time at the discretion of the agency program coordinator. Violation of any term or condition of the memorandum of understanding/confidentiality statement constitutes grounds for de-selection. Non-selection and de-selection are not adverse actions and are neither appealable nor grievable under the NCIS administrative grievance policy.

c. Training. Initial training consists of at least 40 hours of formal instruction in mental illness, suicide, grief, chemical dependency and other compulsive behaviors, counseling skills, listening skills, issues with families and children, critical incidents, trauma, vicarious trauma, anger management, stress management, and referral techniques.

d. Meetings and documentation. The agency program coordinator will ensure peer support responders capture statistical data. This data may include the number and type of program participant contacts but must not contain information that could potentially identify individual program participants. This data will be forwarded to the agency program coordinator and the assistant agency program coordinator on a quarterly basis. The agency program coordinator will use the data to prepare an annual report for the Director on the nature and number of peer support responder contacts. The clinical psychologist (or designee) will attend peer support responder meetings to provide assistance and consultation regarding past and ongoing contacts with program participants. Meetings will also provide opportunities for continuing education.

e. Ethical issues. The behaviors and actions of peer support responders reflect on the credibility of the PSP as a whole. Inappropriate behavior can damage the trust employees place in the program. The integrity of peer support responders, and their respect for each program participant's dignity, self-development, and personal welfare is paramount to maintaining the program's credibility. Ethical lapses may be cause for non-selection or de-selection.

(1) Peer support responders will not exercise power over program participants or derive personal gain from helping them. To avoid creating a conflict of interest, or the perception thereof, peer support responders are prohibited from accepting any gift or remuneration from a program participant, engaging in activities to meet their personal needs at the expense of the program participant, or asking for favors or help from a program participant. A peer support responder's sole reward is the satisfaction of assisting a fellow employee.

(2) In developing trust with a program participant, it is important for peer support responders to explain their role and describe what services can and cannot be offered. Peer support responders are primarily caring and attentive listeners, serving as a bridge to help fellow employees find the professional help or long-term support (EAP, for example) they may need. Peer support responders are not expected to solve the program participants' problems.

(3) Peer support responders must scrupulously avoid dual relationships with program participants. Such dual relationships may include situations in which a program participant and the peer support responder are engaged in an intimate relationship, the program participant and peer support responder are involved in any capacity in the same internal investigation, the program participant's need for peer support stems from an incident involving the peer support

responder or his or her chain of command, and other situations diminishing the peer support responder's ability to remain objective. Peer support responders must strive to be neutral and avoid partisanship or alignment with management or employee organizations. The PSP relies on the trust and endorsement of management and all employees.

(4) Both the peer support responder and program participant maintain the right at all times to terminate the peer support responder-program participant relationship or request that the matter be reassigned to a different peer support responder. Confidentiality of information gained during the peer support responder-program participant relationship survives the termination of that relationship.

f. Confidentiality. Confidentiality of information disclosed by the program participant during peer support sessions is extremely important to the effectiveness and success of the PSP. However, there are limits to the program's ability to keep confidential information provided by program participants during peer support sessions.

(1) Prior to entering into a peer support relationship, peer support responders must inform the program participant that, infrequently and under certain limited circumstances, information obtained during the session may need to be revealed and that, although confidentiality is an important goal of the program, it cannot always be guaranteed.

(2) Instances in which peer support responders may be required[1] to reveal confidential information obtained during a peer support session include the following:

(a) Peer support responder learns information that they are required to report pursuant to the Insider Threat Program and the Counterintelligence Awareness and Reporting (CIAR) directive, described in references (a) and (b).

(b) Peer support responder learns of possible violations of law or policy, including sexual harassment.

(c) Peer support responder learns of threats of violence or harm toward another person or persons and has a "duty to warn."

(d) Peer support responder learns of allegations of suspected child abuse or neglect, or has probable cause to believe that a crime has been committed within a domestic relationship.

(3) Peer support responders who determine a need to reveal confidential information,[1] such as that described in this chapter, must:

(a) Immediately attempt to elicit the program participant's voluntary disclosure to an appropriate individual. If this fails, the peer support responder must attempt to obtain the program participant's express consent for the peer support responder to reveal the information. The program participant's consent constitutes a waiver of confidentiality. When express

[1] Peer support responders who have questions in any particular circumstance about whether reporting is mandatory should immediately consult with the agency program coordinator.

consent is obtained from the program participant, the peer support responder must inform the program participant what disclosures they intend to make and to whom. The peer support responder will provide this information only to those specifically authorized to receive the information—individuals who have a specific need to know for narrowly tailored and legitimate business, safety, security and/or law enforcement purposes.

(b) If the peer support responder believes there is a need to disclose information and the program participant does not voluntarily disclose or provide consent, the peer support responder must report the information to the agency program coordinator. The agency program coordinator will evaluate the information, make inquiries as necessary, determine whether the reported information must be disclosed for a legitimate business, safety, security, or law enforcement purpose and, if so, ensure that the proper entities are contacted and informed. The peer support responder may be required to respond to inquiries from medical, health care, or other professionals, including psychologists and psychiatrists, law enforcement professionals, NCIS, Department of Navy, Department of Defense executives, or inspectors general (including their designees). Without the consent of the program participant, the peer support responder normally will not initiate disclosure to anyone other than the agency program coordinator, except in situations that present an extreme emergency. However, in the event that the agency program coordinator reports an incident of which the peer support responder made him or her aware and other professionals need to discuss the matter with the peer support responder for legitimate business, safety, security, or law enforcement reasons, the peer support responder has a duty to participate and provide responsive information if directed to do so by the agency program coordinator.

(4) Breaching a program participant's confidentiality, other than for safety and legal purposes, is a serious matter and is detrimental to the success of the program, as it violates the trust placed in the peer support responder by the program participant.

(a) The agency program coordinator may remove peer support responders from the PSP if they intentionally and inappropriately breach program participants' confidentiality and/or intentionally deviate from the protocols in this chapter. Removal may not be grieved.

(b) Peer support responders who reveal confidential information about program participants to those without an official need to know or pursuant to a routine use may be subject to penalties under the Privacy Act of 1974.

(c) Peer support responders may be disciplined for failure to follow policies relating to confidentiality and for unauthorized disclosures.

g. Critical Incident Response Team. Peer support responders will be integrated into the Critical Incident Response Team outlined in reference (c) and will provide additional assistance to NCIS personnel involved in a critical incident, augmenting the capabilities of the Civilian Employee Assistance Program (references (d) (e) and (f)).

NCIS-1, CHAPTER 59
OFFICE OF MILITARY SUPPORT ROLES AND RESPONSIBILITIES
EFFECTIVE DATE: JUNE 2015

TABLE OF CONTENTS **PAGE**

Reference:
(a) BUPERS Instruction 1610.10C, Navy Performance Evaluation System, 20 April 2011

59-1. Purpose. To establish roles and responsibilities for the administrative control (ADCON) and operational control (OPCON) of all Navy personnel assigned to the Naval Criminal Investigative Service (NCIS). ADCON of USMC personnel is covered under separate memorandums of agreement and memorandums of understanding between NCIS and the Commandant of the Marine Corps.

59-2. Policy. The Commanding Officer (CO), OMS, maintains ADCON, or exercise of authority over subordinate units in respect to administration and support, including personnel management, readiness, and discipline of all Navy personnel assigned to NCIS. The assigned NCIS supervisor has OPCON over individuals assigned to them and is responsible for their daily activities, to include assignment of tasks, evaluation of daily performance, job-related training, firearms qualification, quality control of products, and professional development.

a. Administrative control. CO, OMS, is responsible for administration and military readiness of all military personnel assigned to NCIS units worldwide, regardless of location or operational mission. In order to effectively perform this function, all military personnel are assigned to OMS and detailed to specific NCIS codes or field offices to perform operational missions. CO, OMS, will issue additional policy as necessary to facilitate ADCON and to maintain good order and discipline.

b. Routine administrative and military matters. CO, OMS, maintains approval authority for routine administrative and military matters. These items include assignments, evaluations and fitness reports, military awards, personnel action requests including NAVPERS 1070/1306 requests, overseas tour extension incentive program requests, projected rotation date extensions, reenlistment requests, early release from active duty, officer resignations, civilian clothes authorizations, waivers to grooming standards, separation and transfer, formal disciplinary action, career counseling, physical fitness assessment, professional military education, urinalysis, leave and liberty, accountability, and military-related training.

c. Reserves. CO, OMS, maintains OPCON over NCIS reserve units to ensure they are trained, equipped, and postured to support NCIS as the mission dictates. For units that are collocated with a field office, the Special Agent in Charge (SAC) retains the ability to train

reservists in coordination with OMS via the unit CO or Officer in Charge (OIC) and the Operational Support Officer (OSO) and utilize personnel for contributory support to regional missions as the SAC sees fit. OMS personnel are enterprise assets and may be used to support various NCIS missions.

d. Legal authority. CO, OMS, is the special courts-martial convening authority and non-judicial punishment authority within NCIS. CO, OMS, must be notified immediately about incidents that may require administrative or disciplinary action against any Navy personnel assigned to NCIS.

e. Award recommendations. To enhance timely recognition of deserving personnel while upholding U.S. Navy standards, CO, OMS, reviews and approves all award recommendations for Navy personnel assigned to NCIS. This review and approval includes input in any manner to awarding authorities outside of NCIS. This includes the Navy awards board, or in the case of the Secretary of the Navy (SECNAV), Chief of Naval Operations (CNO), or Commandant of the Marine Corps (CMC) for non-directed awards. Awards recommended by SECNAV, CNO, or CMC will be expedited by OMS. CO, OMS is the approval authority for Navy and Marine Corps Commendation Medals and below. Award recommendations for Meritorious Service Medals and above will be forwarded to the Director, NCIS via the CO OMS for concurrence/endorsement prior to being submitted to the Secretary of the Navy Awards Board for consideration. The Secretary of the Navy is the awarding authority for Meritorious Service Medals for Navy personnel assigned to NCIS. No further sub-delegation is authorized.

f. Screenings and assignments. OMS maintains liaison with Bureau of Naval Personnel detailers, placement officers, and community managers for the proper screening and assignment of all candidates recommended for assignment to NCIS.

g. Senior military officers. CO, OMS, may appoint military officers and senior enlisted personnel throughout NCIS to oversee the administrative and military readiness of all Navy personnel within their area of responsibility, as defined by CO, OMS. These duties are in addition to those officers and senior enlisted personnel's operational duties or other duties that may be assigned by the SAC or other NCIS supervisor.

59-3. Cancellation. Gen Admin 11-0023, NCIS Policy Document No.11-12: Personnel (Processing of Enlisted and Chief Evaluations, Officer Fitness Reports, and Awards for Active Duty Personnel Assigned to NCIS worldwide, 28 June 2011.

59-4. Chapter Sponsor. Office of Military Support, Code 0MS.

APPENDIX A
EVALUATION POLICY

1. This evaluation policy provides direction for processing enlisted evaluations, chief evaluations, and officer fitness reports for all active-duty Navy personnel assigned to the Naval Criminal Investigative Service (NCIS). Reference (a) provides guidance on the preparation of all performance evaluations.

2. Timely and accurate processing of performance evaluations is essential to the proper evaluation management of all active-duty Navy personnel assigned to NCIS.

3. Unless otherwise specified by the Director, NCIS, CO, OMS, is the reporting senior for all active-duty Navy personnel assigned to NCIS.

a. All enlisted evaluations, chief evaluations, and officer fitness reports will be prepared in draft by the operational chain of command and forwarded to CO, OMS. CO, OMS, will coordinate any substantive changes in the final report with the operational chain of command.

b. CO, OMS, may delegate, in writing, the signing of enlisted evaluations, chief evaluations, and officer fitness reports, in accordance with reference (a).

c. Block 26 on all enlisted evaluations, chief evaluations, and officer fitness reports will contain UIC 63285, regardless of who will sign as reporting senior.

d. All enlisted evaluations, chief evaluations, and officer fitness reports containing "adverse matter," as defined in reference (a), will be coordinated with and approved by CO, OMS.

e. Delegated reporting seniors who do not have a senior Navy officer (O-4 and above) will forward all officer fitness reports, prior to their being signed by the reporting senior, to CO, OMS, for an administrative review. Delegated reporting seniors who do not have a senior Navy officer or a senior enlisted leader (E-9) will forward all chief evaluations, prior to being signed by the reporting senior, to CO, OMS, for an administrative review. This review will ensure Navy administrative requirements are met and that the spirit and intent of the evaluation and fitness report system are maintained. Reports must be provided electronically to the Executive Officer, OMS, or Command Master Chief, OMS, as applicable, at least 21 days before the end of the reporting period.

4. To provide a centralized filing system for command administrative purposes and to ensure equitable standards are used throughout NCIS, a copy of all enlisted evaluations, chief evaluations, and officer fitness reports not signed by CO OMS will be retained by NCIS field offices or STAAT, as applicable. Field offices and STAAT will forward copies of all Navy evaluations and fitness reports to OMS Admin. OMS Admin will retain copies of all enlisted evaluations, chief evaluations, and officer fitness reports signed by CO OMS.

NCIS-1, CHAPTER 60
OFFICIAL NCIS SOCIAL MEDIA SITES
EFFECTIVE DATE: AUGUST 2015

TABLE OF CONTENTS **PAGE**

References:

(a) DoD Instruction 8550.01, DoD Internet Services and Internet-Based Capabilities, 11 September 2012
(b) ALNAV 056/10, Internet-Based Capabilities Guidance–Official Internet Posts, August 2010
(c) Navy Command Leadership Social Media Handbook, Fall 2012
(d) NCIS Employees' Guide to Standards of Conduct, Legal Office (00LJ), July 2014
(e) NCIS-1, Chapter 27, NCIS Information Technology, December 2006
(f) NCIS Anti-Harassment Policy Statement, February 2015

60-1. Purpose. This chapter establishes policy on the use, management, and oversight of NCIS official social media sites and posts by NCIS personnel acting in an official capacity.

60-2. Policy. NCIS endorses the secure use of social media to enhance communication, collaboration, and information exchange; streamline processes; and foster productivity. Social media is an integral part of the strategic communication and public affairs mission of NCIS. Official NCIS social media accounts are centrally managed by the Communications Directorate. The Communications Director will establish and maintain all official NCIS social media accounts for the agency. At the discretion of the SAC, a field office may operate an official NCIS field office Facebook account. Field offices are not authorized to establish any other social media (YouTube, Twitter, Instagram, Pinterest, etc.) accounts. No other NCIS element is authorized to establish, maintain, or operate any social media account. All official social media posts and accounts must adhere to the social media aspects of the policies found in references (a) through (f).

60-3. Cancellation. None

60-4. Chapter sponsor. Communications Directorate, Code 00C.

60-5. Responsibilities

a. The Communications Directorate, Code 00C. Acts as the subject matter expert on official NCIS social media accounts and creates and oversees all official NCIS social media accounts. Code 00C will:

(1) Create and maintain an agency-wide Facebook account for NCIS and an official NCIS YouTube Channel.

(2) Represent NCIS and establish official accounts on other social media platforms as deemed necessary by the NCIS Director of Communications.

(3) Create field office Facebook accounts, establish logon information, and provide usernames and passwords to the field office special agents in charge (SACs) and account managers.

(4) Ensure all official NCIS social media sites are appropriately registered with DoD, DON, and CHINFO to comply with the U.S. Navy Social Media User Agreement per references (a) and (c).

b. SACs. If the SAC desires an official NCIS field office Facebook page, the SAC will submit a request, with concurrence from the Executive Assistant Director, to the Communications Directorate. The request form is posted on the shared 00C site on Lighthouse. The SAC will:

(1) Assign an account manager and notify Code 00C.

(2) Create content for field office Facebook page that complies with this policy.

(3) Monitor and ensure all posts and content on the field office Facebook page comply with this policy and are screened for threats, leads, and other items of interest. Report violations and concerns to appropriate channels and advise Code 00C.

(4) Consider coordinating, in consultation with Code 00C, with local commands to link to and network with other official Facebook accounts.

(5) Notify Code 00C regarding changes in account managers.

(6) Submit recommended content for NCIS Facebook page to the Communications Directorate.

c. Field office Facebook account managers and alternates. May create content for the field office Facebook page and is responsible for ensuring that information posted is appropriate, is written in such a manner that a reasonable reader would understand that the comments are being made on behalf of the agency, and adheres to this policy. Conduct themselves as representatives of the agency at all times, adhere to all agency standards of conduct, and observe conventionally accepted protocols and proper decorum. Monitor their sites to be aware of posted comments, immediately record and hide inappropriate comments (those using profanity or making threats) and promptly notify Code 00C. Account managers also will:

(1) Review all posted topics and reasonable comments; correct misinformation in a respectful, clear, and concise manner; and avoid personal attacks. If assistance is needed, contact 00C for guidance.

(2) Ensure, to the best of their ability, that information posted on field office Facebook accounts is not law enforcement sensitive, proprietary, privileged, copyrighted, or trademarked.

(3) Ensure information posted on field office Facebook accounts does not violate operational security, personally identifiable information (PII) guidelines, or classified material regulations.

(4) Coordinate with Code 00C on information for public release regarding ongoing investigations or operations for approval by NCIS Deputy Director prior to posting.

(5) Coordinate with Code 00C for review and approval before posting any agency personnel lists, charts, or directories that provide names, addresses or telephone numbers of individuals.

(6) Maintain a spreadsheet to log all material posted to their field office Facebook page, including date of post, exact text of post, author of post, date and text of links posted, and comments made by page administrators.

(7) Refrain from posting information that is political, implies endorsement of non-federal entity products or services, or links to an entity that may imply endorsement, such as a charitable site.

(8) Refrain from posting statements about the guilt or innocence of any suspect or arrestee or comments regarding pending prosecutions.

(9) Refrain from transmitting or otherwise disseminating confidential information, including photographs or videos.

(10) Be mindful of potential undercover assignments, operational security, and privacy issues and refrain from posting images of NCIS special agents or professional staff without their permission.

(11) Ensure all posted links are related to appropriate external articles or websites.

d. All other NCIS elements may submit content with the approval of the SAC or AD to Code 00C for inclusion on the official NCIS Facebook page.

60-6. Instructional Guides. Facebook account instructional guides are posted on the 00C Lighthouse page for field office Facebook account managers and alternates who need training and guidance on the use of Facebook and its basic functions.

NCIS-1, CHAPTER 62
OFFICE OF THE OMBUDSMAN
EFFECTIVE DATE: AUGUST 2015

TABLE OF CONTENTS **PAGE**

References

(a) Presidential Memorandum, Designation of Interagency Committees to Facilitate and Encourage Agency Use of Alternative Means of Dispute Resolution and Negotiated Rulemaking, May 1, 1998
(b) DoD Directive 5145.5, Alternative Dispute Resolution, April 22, 1996
(c) SECNAVINST 5800.13A, Alternative Dispute Resolution (ADR) Policy and Mission of the DON ADR Program Office, December 22, 2005

62-1. Purpose. The purpose of this chapter is to outline the NCIS Office of the Ombudsman roles and responsibilities and provide guidance for NCIS management personnel involved with the NCIS Office of the Ombudsman.

62-2. Policy. The NCIS Office of the Ombudsman is predicated upon years of experience in identifying and resolving work related matters at the lowest levels; to the benefit of both employee and employer in accordance with references (a), (b), and (c). NCIS will provide the services of the Office of the Ombudsman to all employees as an informal means in an effort to resolve work-related issues. Employees will not face retaliation for consulting with the Ombudsman or seeking the services of the Office of the Ombudsman. Contact information is available on the Ombudsman page on Lighthouse:

(b)(7)(E)

a. The NCIS Office of the Ombudsman is an independent, impartial, and confidential resource for all personnel seeking early resolution of workplace-related concerns. The ombudsman will endeavor to keep all matters and consultations with managers and employees confidential to the greatest extent possible, unless the manager or employee agrees to disclosure; however, there is no guarantee of confidentiality. There may be instances where there the ombudsman has a duty to report illegal or suspicious behavior for legitimate business, safety, security, or law enforcement reasons. All activities will be conducted in accordance with the International Ombudsman Association Standards of Practice (available on the Office of the Ombudsman page on Lighthouse).

b. The office neither acts as an agent for, nor accepts notice on behalf of, the DoD or NCIS and does not serve in a position or role that is designated by the Agency as a place to receive notice on behalf of the Agency.

c. NCIS will not tolerate any form of retaliation against an employee for contacting the Office of the Ombudsman and appropriate disciplinary measures will be taken in instances in which a supervisor or Agency official is found to have retaliated.

62-3. Cancellation. None.

62-4. Chapter Sponsor. Office of the Ombudsman.

62-5. Responsibilities

a. The Director will:

(1) Appoint an employee to serve as ombudsman.

(2) Provide sufficient resources for the ombudsman to fulfill the responsibilities enumerated herein.

b. The ombudsman/deputy ombudsman will:

(1) Obtain relevant education and training.

(2) Receive complaints, concerns, and questions about alleged acts, omissions, improprieties, and systemic problems within the NCIS.

(3) Address employee complaints, concerns or questions in a fair manner.

(4) Gather relevant information as needed.

(5) Address employee complaints, concerns, and questions at the most appropriate supervisory level.

(6) Use a variety of methods to pursue resolution of complaints and concerns by:

(a) Conducting informal inquiries.

(b) Developing, evaluating, and discussing options to resolve problems, address concerns, and facilitate communication among employees.

(7) Educate and train employees in conflict resolution to amicably resolve issues.

(8) Identify complaint patterns and trends.

(9) Provide complaint metrics and trends annually to the Director.

(10) Report ADR techniques used annually to the DON ADR program office.

(11) Move issues to the appropriate level in the event they are not within the ombudsman's jurisdiction to attempt to resolve them. For instance, reports of EEO issues should be coordinated with the EEO Office. In the event that an NCIS employee reports an issue containing an EEO component or possible EEO component to the ombudsman, the ombudsman will inform the employee that EEO issues must be discussed with an NCIS EEO Counselor in the EEO Office. Contacting the ombudsman does not substitute for timely contact with an EEO Counselor to report discrimination or retaliation as required by 29 C.F.R. §1614.105(a)(1).

(12) The Ombudsman will not:

(a) Make, change, or set aside a law, policy, or administrative decision.

(b) Make binding decisions or determine employee rights.

(c) Compel NCIS employees to implement the ombudsman's recommendations.

(d) Conduct investigations that substitute for administrative or judicial proceedings.

(e) Accept jurisdiction over an issue that is pending in a legal forum unless all parties and the presiding officer in that action explicitly consent.

c. NCIS managers will:

(1) Cooperate and share information with the ombudsman in accordance with law and security requirements

(2) Encourage a positive dispute resolution climate through appropriate conflict management practices consistent with DoD and NCIS policies.

(3) Encourage personnel to address conflicts early and at the lowest possible level.

1990934 11:51 20150911 IN:SSDEMAIL #1 OUT:NCISWWSSD #1

GENERAL ADMINISTRATION 11SEP15

FROM: 002G GEN: 02G-0007

TO: DIST

SUBJ: NCIS-2/KEY PERSONNEL GLOBAL OPERATIONS (002G)

02G GLOBAL OPERATIONS

Executive Assistant Director (02G)

(b)(6)

Executive Assistant/Resident Agent in Charge Of Forensics and TSCM (02G) Elizabeth Toomer

(b)(6)

Senior Intel Officer (02G)

(b)(6)

Desk Officer (02G)

(b)(6)

Executive Staff Assistant (02G)

(b)(6)

OFFICE OF SPECIAL PROJECTS (OSP)
Special Agent in Charge

(b)(6)

FOR OFFICIAL USE ONLY
PAGE 1

11SEP15

SUBJ: NCIS-2/KEY PERSONNEL GLOBAL OPERATIONS (002G)

OFFICE OF STRATEGIC SUPPORT (OSS)
Special Agent in Charge

(b)(6)

CONTINGENCY RESPONSE FIELD OFFICE (CRFO) Resident Agent in Charge Cathy Clements

(b)(6)

CYBER OPERATIONS FIELD OFFICE (CBFO)
Special Agent in Charge

(b)(6)

PROTECTIVE OPERATIONS FIELD OFFICE (POFO) Special Agent in Charge Brian Curley

(b)(6)

(b)(6)

POLYGRAPH FIELD OFFICE (2GVQ)
Special Agent in Charge

(b)(6)

OFFICE OF TECHNICAL SURVEILLANCE
COUNTER MEASURES (TSCM/2GJQ)
Security Specialist in Charge

(b)(6)

OFFICE OF FORENSIC SUPPORT (2GFS)
Forensics Specialist in Charge

(b)(6)

11SEP15

SUBJ: NCIS-2/KEY PERSONNEL GLOBAL OPERATIONS (002G)

OFFICE OF TECHNICAL SERVICES (2GTS)
Resident Agent in Charge

(b)(6)

DISTRIBUTION:
NCISHQ: WWHQ
INFO: WWSSD/AFLT

GENERAL ADMINISTRATION 11FEB16

FROM: 2AZL GEN: ZL-0001

TO: DIST

SUBJ: NCIS-2/(2AZL) STAAT LANT AND DETACHMENT KEY PERSONNEL DATA SHEET

MAILING ADDRESS LOCAL ADDRESS
1430 HELICOPTER RD STE 250 BLDG 3801 JEB LITTLE CREEK-FORT STORY
VA BEACH, VA 23459-2929 1430 HELICOPTER RD STE 250
VA BEACH, VA 23459-2929

DMS PLA: NAVCRIMINVSERV STAAT NORFOLK VA//2AZL//

STAATLANT REGION VA BEACH (2AZL)

PERSONNEL	TITLE	OFFICE	DSN
(b)(6)			

STAATLANT DET NORFOLK (2AZN)

(b)(6)

FOR OFFICIAL USE ONLY
PAGE 1

11FEB16

SUBJ: NCIS-2/(2AZL) STAAT LANT AND DETACHMENT KEY PERSONNEL DATA SHE

(b)(6)

STAATLANT DET VA BEACH (2AZV)

(b)(6)

STAATLANT DET SOUTHEAST (2AZM)

(b)(6)

STAATLANT DET EUROPE AND AFRICA (2AZE)

(b)(6)

STAATLANT DET MIDDLE EAST (2AZB)

(b)(6)

DISTRIBUTION
INFO: WWSSD

FOR OFFICIAL USE ONLY
PAGE 2 LAST (b)(6)

GENERAL ADMINISTRATION 12FEB16

FROM: 2AZL GEN: ZL-0002

TO: DIST

SUBJ: NCIS-2/(2AZM) STAAT LANT MAYPORT DETACHMENT DATA SHEET

MAILING ADDRESS	LOCAL ADDRESS
PO BOX 280076	BLDG 1576
NAVAL STATION	MASSEY AVENUE
JACKSONVILLE FL 32228-0076	MAYPORT FL 3228-006

TELEPHONES	COMMERCIAL	DSN
OFFICE	(904) 270-5828	312-370-5828
UNCLAS FAX	(904) 270-6050	312-270-6050

MSG PLA: NAVCRIMINVSERVFO SOUTHEAST MAYPORT FL OFFICE CODE: 2AZM
UIC: 42933

TERRITORIAL COVERAGE:
ALABAMA, FLORIDA, GEORGIA, LOUISIANA, MISISSIPPI, AND TENNESSEE; THE CARIBBEAN, SOUTH AMERICA AND CENTRAL AMERICA (WITH THE EXCEPTION OF MEXICO).

DISTRIBUTION
INFO: WWSSD

FOR OFFICIAL USE ONLY
PAGE 1 LAST (b)(6)

GENERAL ADMINISTRATION 12FEB16

FROM: 2AZL GEN: ZL-0003

TO: DIST

SUBJ: NCIS-2/(2AZV) STAAT LANT VA BEACH DETACHMENT DATA SHEET

MAILING ADDRESS LOCAL ADDRESS
1430 HELICOPTER RD STE 250 BLDG 3801 JEB LITTLE CREEK-FORT STORY
VA BEACH, VA 23459 1430 HELICOPTER RD STE 250
VA BEACH, VA 23459

TELEPHONES COMMERCIAL DSN
OFFICE (757) 462-8925/7893 (312)253-8925/7893
UNCLAS FAX (757) 462-4997

MSG PLA: NAVCRIMINVSERV STAAT NORFOLK VA OFFICE CODE: 2AZV
UIC: 63055

TERRIORIAL COVERAGE:
CONNECTICUT, ILLINOIS, INDIANA, KENTUCKY, MAINE, MASSACHUSETTS, MICHIGAN, NEW HAMPSHIRE, NEW JERSEY, NEW YORK, OHIO, PENNSYLVANIA, RHODE ISLAND, VERMOUNT, AND WISCONSIN.
EASTERN CANADA TO INCLUDE: PROVINCES OF ONTARIO, QUEBEC, NEW BRUNSWICK, NEWFOUNDLAND, NOVA SCOTIA AND PRINCE EDWARD ISLAND.
DISTRICT OF COLUMBIA: ALL AREAS
MARYLAND COUNTIES: ALLEGANY, CHARLES, FREDERICK, GARRETT, PRINCE GEORGE'S, WASHINGTON
VIRGINIA COUNTIES: ARLINGTON, CAROLINE, CLARKE, CULPEPPER, ESSEX, FAIRFAX, FAUQUIER, FREDERICK, GREENE, KING GEORGE, LANCASTER, LOUDOUN, MADISON, NORTHCUMBERLAND, ORANGE, PAGE, PRINCE WILLIAM, RAPPAHANNOCK, RICHMOND, ROCKINGHAM, SHENANDOAH, SPOTSYLVANIA, STAFFORD, WARREN, WESTMORELAND.
WEST VIRGINIA COUNTIES: BARBOUR, BERKELEY, DODD RIDGE, GRANT, HAMPSHIRE, HARDY, HARRISON, JEFFERSON, MARION, MINERAL, MONONGALIA, MORGAN, PLEASANTS, PRESTON, RITCHIE, TAYLOR, TUCKER, TYLER, WETZEL, WOOD.

DISTRIBUTION
INFO: WWSSD

FOR OFFICIAL USE ONLY
PAGE 1 LAST (b)(6)

2301709 11:33 20160120 IN:SSDEMAIL #7 OUT:NCISWWSSD #4

GENERAL ADMINISTRATION 15JAN16

FROM: 2GJQ GEN: 02G-0001

TO: DIST

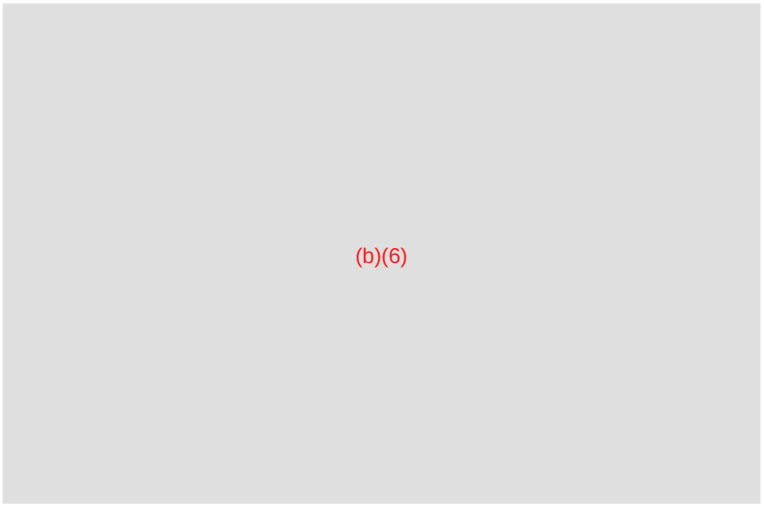
SUBJ: NCIS-2: COUNTERINTELLIGENCE TECHNICAL SERVICES KEY PERSONNEL
DATA SHEET

MAILING ADDRESS:
NAVAL CRIMINAL INVESTIGATIVE SERVICE HEADQUARTERS CODE 2GJQ RUSSELL KNOX BUILDING
27130 TELEGRAPH ROAD
QUANTICO VA 22134-2253

ALL EMAILS SHOULD BE ADDRESSED TO: (b)(6) ncis.navy.smil.mil
STE: 571-305-9160

TITLE CONTACT INFORMATION

(b)(6)



FOR OFFICIAL USE ONLY
PAGE 1

15JAN16

SUBJ: NCIS-2: COUNTERINTELLIGENCE TECHNICAL SERVICES KEY PERSONNEL D

HAWAII
MAILING ADDRESS:
NCIS HAWAII
ATTN Code 2GJV
449 SOUTH AVE
PEARL HARBOR HI 96860

NORFOLK
MAILING ADDRESS:
NCIS OCEANA
ATTN CODE 2GJT
1801 TOMCAT BLVD

VIRGINIA BEACH VA 23460

(b)(6)

SAN DIEGO
MAILING ADDRESS:
NCIS SAN DIEGO
ATTN CODE 2GJU
3405 WELLES ST STE 1
SAN DIEGO CA 92136

(b)(6)

ALL DISCUSSIONS OF PENDING TSCM REQUESTS, SCHEDULING AND INVESTIGATIVE PROCEDURES ARE CLASSIFIED MINIMUM SECRET/NOFORN PER DODINST 5240.05

2202722 17:23 20151208 IN:SSDEMAIL #3 OUT:NCISWWSSD #1

GENERAL ADMINISTRATION 08DEC15

FROM: 2PZP GEN: ZP-0003

TO: DIST

SUBJ: NCIS-2: (2PZP) NCIS SECURITY TRAINING, ASSISTANCE, ASSESSMENT
TEAM PACIFIC FIELD OFFICE KEY PERSONNEL

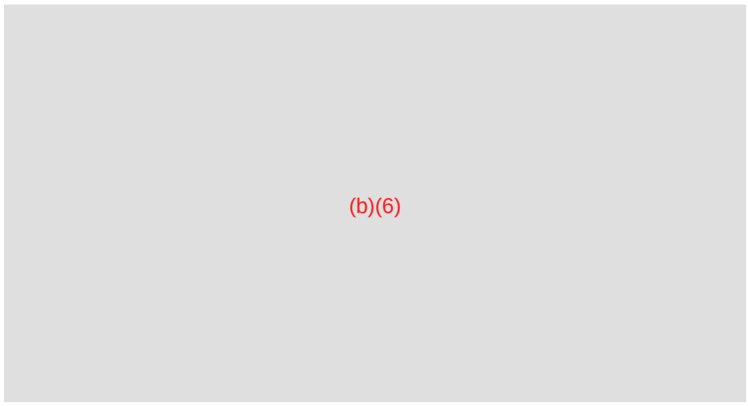
MAILING ADDRESS LOCAL ADDRESS
SECURITY SPECIALIST IN CHARGE BUILDING 91 ROOSEVELT BLVD
PO BOX 357053 NAVAL BASE CORONADO
SAN DIEGO CA 92135-7053 SAN DIEGO CA 92135-7053

TELEPHONES: COMMERCIAL: (CONUS 011) DSN: 312
OFFICE (619) 545-9427/8934 735/577
AFTER HOURS (619) 204-1116(LCDR (b)(6)
OPERATIONS OFFICER)
UNCLAS FACSIMILE (619) 545-6166 735-6166
STE (619) 767-7874 577-7874

STAAT PAC PERSONNEL (UIC) 63057

SECURITY SPECIALIST IN CHARGE

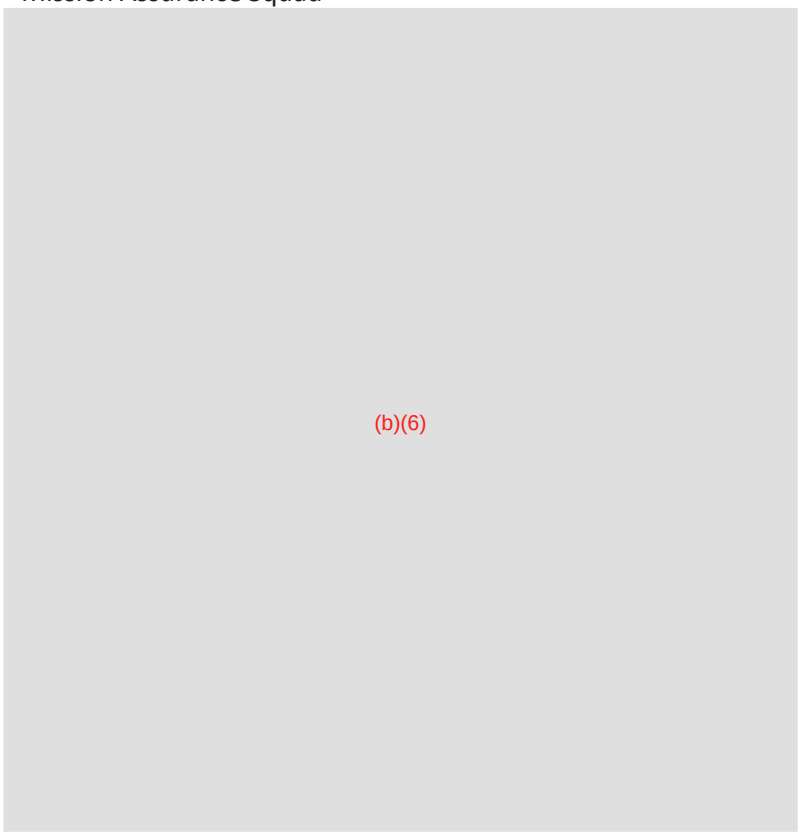
(b)(6)



08DEC15

SUBJ: NCIS-2: (2PZP) NCIS SECURITY TRAINING, ASSISTANCE, ASSESSMENT

Mission Assurance Squad



(b)(6)

STAAT PAC SINGAPORE DETACHMENT (UIC) 40484 DSN: (b)(6)

(b)(6)

STAAT PAC YOKOSUKA DETACHMENT (UIC) 0765A DSN: (b)(6)

(b)(6)

STAAT PAC MANILA UNIT

(b)(6)

DMS: PLA: NAVCRIMINVSERV STAAT SAN DIEGO CA//2PZP//

SSD ELECTRICAL DISTRIBUTION CODE: /2PZP//

SUBORDINATE OFFICES:

STAAT PAC NORTHWEST DETACHMENT (2PZA)
STAAT PAC SINGAPORE DETACHMENT (2PZS)
STAAT PAC MANILA UNIT (2PZI)

08DEC15

SUBJ: NCIS-2: (2PZP) NCIS SECURITY TRAINING, ASSISTANCE, ASSESSMENT

STAAT PAC FAR EAST DETACHMENT (2PZY)

TERRITORIAL COVERAGE:

THE GEOGRAPHICAL AREA OF RESPONSIBILITY OF NCIS STAAT PAC INCLUDES AREAS ASSIGNED TO NCIS SOUTHWEST FIELD OFFICE, NORTHWEST FIELD OFFICE, SINGAPORE FIELD OFFICE, FAR EAST FIELD OFFICE, HAWAII FIELD OFFICE, AND MARINE CORPS WEST FIELD OFFICE.

ADDRESSES FOR STAAT PAC OFFICES:

NCIS STAAT SAN DIEGO FIELD OFFICE
P O BOX 350753
SAN DIEGO CA 92135-7053

OR

NAVAL BASE CORONADO
ROOSEVELT MURRAY ROAD
BUILDING 91
SAN DIEGO, CA 92135-7053

NCIS STAAT PACNORWEST OFFICE
ATTN SSS KEN TRANTHAM
1003 SUNFISH DRIVE
SILVERDALE WA 98315-9622

NCIS FAR EAST FIELD OFFICE
ATTN SSS JOE ST CYR
PSC 473 BOX 76
FPO AP 96349-0076

OR

NCIS STAAT FAR EAST OFFICE
BUILDING 39A 2F YOKOSUKA NAVAL BASE
1 HON-CHO YOKOSUKA-SHI
KANAGAWA 2380041 JAPAN

OR FOR FED EX

NCIS FAR EAST FIELD OFFICE
BUILDING 1997 2F YOKOSUKA NAVAL BASE
1 HON-CHO YOKOSUKA-SHI
KANAGAWA 2380041 JAPAN

NCIS SINGAPORE OFFICE
ATTN SSS JONATHAN GREENSTEIN
PSC 470 BOX 290
FPO AP 96534-2900

08DEC15

SUBJ: NCIS-2: (2PZP) NCIS SECURITY TRAINING, ASSISTANCE, ASSESSMENT

OR

FLEET LOGISTIC CENTER YOKOSUKA
SITE SINGAPORE
PSA SEMBAWANG TERMINAL
DEPTFORD ROAD BLDG-7-4
SINGAPORE 759657
M/F: (b)(6)

NCISRA MANILA OFFICE
ATTN OSCAR POLK
UNIT 8600 BOX 1434
DPO AP 96515-1434

OR
CHANCERY BUILDING
AMERICAN EMBASSY MANILA
1201 ROXAS BLVD., ERMITA
MANILA, 1000, PHILIPPINES

DISTRIBUTION:
//WWSSD//

FOR OFFICIAL USE ONLY
PAGE 4 LAST (b)(6)

21AUG09

NCIS-2: (0021) COMBATING TERRORISM DIRECTORATE KEY PERSONNEL DATA SHEET

MAILING ADDRESS
NAVAL CRIMINAL INVESTIGATIVE SERVICE
HEADQUARTERS (NCISHQ CODE 0021)
716 SICARD ST., SE, SUITE 2000
WASHINGTON NAVY YARD, BLDG 111
WASHINGTON, DC 20388-5380

TELEPHONES
DSN PREFIX: 288/325 FOR 685 NUMBERS
OFFICE: 202-433-9077
UNCLASS FAX: 202-433-9147
CLASS FAX: 202-433-9194

CODE/PERSONNEL	TELEPHONE NUMBERS
21 COMBATING TERRORISM DIRECTORATE	
EXECUTIVE ASSISTANT DIRECTOR (b)(6)	OFFICE: CELL:
21A PROGRAM DIRECTION DEPARTMENT	
DEPUTY ASSISTANT DIRECTOR (b)(6)	OFFICE: CELL: HOME:
DIVISION CHIEF (b)(6)	OFFICE: CELL: HOME:
SUPERVISORY SPECIAL AGENT (b)(6)	OFFICE: CELL:
STATE DEPT REPRESENTATIVE (b)(6)	OFFICE: CELL: HOME:
BUDGET/TRAVEL VACANT TEMP POC LISA FUSCO	OFFICE: CELL:
LEAD INVESTIGATIONS REVIEW SPECIALIST (b)(6)	OFFICE: CELL:
21A1 PHYSICAL SECURITY/ANTI-TERRORISM DIVISION	
DIVISION CHIEF (b)(6)	OFFICE: CELL:
STAAT TRAINING PROGRAM MANAGER VACANT	OFFICE: CELL: HOME

(b)(6)

STAAT CNOIVA PROGRAM MANAGER
(b)(6)
OFFICE:
CELL:
HOME:

STAAT MSC-ISA PROGRAM MANAGER
(b)(6)
OFFICE:
CELL:
HOME:

STAAT PIVA PROGRAM MANAGER
(b)(6)
OFFICE:
CELL:
HOME:

DESK OFFICER (FPD MATTERS)
(b)(6)
OFFICE:
CELL:
HOME:

(b)(6)

21B CT OPERATIONS AND INVESTIGATIONS DEPARTMENT

DEPUTY ASSISTANT DIRECTOR
(b)(6)
OFFICE:
CELL:
HOME:

NJTTF DEPUTY UNIT CHIEF
TBD
OFFICE: TBD
CELL: TBD
HOME: TBD

DIVISION CHIEF, SENIOR REP - FBIHQ, CTD
INTERNATIONAL TERRORISM OPERATIONS SECTION
(b)(6)
OFFICE:
CELL:
HOME:

OARDEC REPRESENTATIVE
(b)(6)
OFFICE:
CELL:
HOME:

21B PACIFIC DIVISION

DIVISION CHIEF
(b)(6)
OFFICE:
CELL:

LNO SPECIAL OPERATIONS COMMAND (SOCOM)
(b)(6)
OFFICE:
HOME:

LNO CENTRAL COMMAND (CENTCOM)
(b)(6)
OFFICE:
CELL:

(b)(6)

21B ATLANTIC DIVISION

DIVISION CHIEF
(b)(6)
OFFICE:
CELL:
HOME:

SUPERVISORY SPECIAL AGENT OPS/INV
(b)(6)
OFFICE:
CELL: TBD

CT ANALYTICAL DIVISION CHIEF
(b)(6)
OFFICE:
CELL:
HOME:

21B1 PROTECTIVE OPERATIONS DEPARTMENT

DEPUTY ASSISTANT DIRECTOR
(b)(6)
OFFICE:
CELL:
HOME:

PERSONAL SECURITY ADVISOR CMC
(b)(6)
OFFICE:
CELL:
HOME:

PERSONAL SECURITY ADVISOR CNO
(b)(6)
OFFICE:
CELL:

PERSONAL SECURITY ADVISOR SECNAV
(b)(6)
OFFICE:
CELL:
HOME:

PERSONAL SECURITY ADVISOR CJCS
(b)(6)
OFFICE:
CELL:
HOME:

OPERATIONS OFFICER
(b)(6)
OFFICE:
CELL:
HOME:

SSA PROTECTIVE SERVICE OPERATIONS
(b)(6)
OFFICE:
CELL:
HOME:

(b)(6)

21B CRIMINAL INVESTIGATIVE TASK FORCE (CITF) FT. BELVOIR

SPECIAL AGENT IN CHARGE
(b)(6)
OFFICE:
CELL:

ASSISTANT SPECIAL AGENT IN CHARGE
(b)(6)
OFFICE:
CELL:
HOME:

SUPERVISORY SPECIAL AGENT
(b)(6)
OFFICE:
CELL:
HOME:

(b)(6)

1457013 10:49 20150226 IN:SSDEMAIL #2 OUT:NCISWWSSD #2

GENERAL ADMINISTRATION 26FEB15

FROM: 0022 GEN: 22-0003

TO: DIST

SUBJ: NCIS-2 (0022) NATIONAL SECURITY DIRECTORATE KEY PERSONNEL
DATA SHEET

MAILING ADDRESS
NAVAL CRIMINAL INVESTIGATIVE SERVICE
HEADQUARTERS (NCISHQ CODE 0022)
27130 TELEGRAPH ROAD
QUANTICO, VA 22134

TELEPHONES
DSN PREFIX: INCOMING 240-XXXX (LAST 4)
OUTGOING 94-XXX-XXXX (CONUS)
OUTGOING 94-312-XXX-XXXX (OCONUS)
OFFICE: 571-305-9689 (TEMP)
UNCLASS FAX: 571-305-9574
SECURE FAX: 571-305-9575

NAVMSG PLA: NAVCRIMINVSERVHQ NSD QUANTICO VA

CODE/PERSONNEL TELEPHONE NUMBERS

EXECUTIVE ASSISTANT DIRECTORATE OFFICE: (b)(6)
(b)(6)

ASSISTANT DIRECTOR OFFICE: (b)(6)
(b)(6)

SENIOR POLICY ADVISOR OFFICE: (b)(6)
(b)(6)

STATE DEPARTMENT REPRESENTATIVE OFFICE: (b)(6)
(b)(6)

DEPUTY UNDER SECRETARY DEFENSE INTEL OFFICE: (b)(6)
(b)(6)

JOINT STAFF CCICA OFFICE: (b)(6)
(b)(6)

22A PROGRAM DIRECTION

DEPUTY ASSISTANT DIRECTOR OFFICE: (b)(6)
(b)(6)

SENIOR PROGRAM ANALYST OFFICE: (b)(6)
(b)(6)

FOR OFFICIAL USE ONLY
PAGE 1

26FEB15

SUBJ: NCIS-2 (0022) NATIONAL SECURITY DIRECTORATE KEY PERSONNEL DATA

DIVISION CHIEF OFFICE: (b)(6)
(b)(6)

SUPERVISORY SPECIAL AGENT PROGRAMS/POLICY OFFICE: (b)(6)
(b)(6)

FPD PROGRAM MANAGER OFFICE: (b)(6)
(b)(6)

FOSO OFFICE: (b)(6)
(b)(6)

22B INVESTIGATIONS

DEPUTY ASSISTANT DIRECTOR OFFICE: (b)(6)
(b)(6)

DIVISION CHIEF OFFICE: (b)(6)
(b)(6)

SUPERVISORY SPECIAL AGENT INV OFFICE: (b)(6)
(b)(6)

DIVISION CHIEF INSIDER THREAT OFFICE: (b)(6)
(b)(6)

SUPERVISORY SPECIAL AGENT INSIDER THREAT OFFICE: (b)(6)
(b)(6)

LNO N2N6 OFFICE: (b)(6)
(b)(6)

NJTTF DEPUTY UNIT CHIEF OFFICE: (b)(6)
(b)(6)

STAFF PSYCHOLOGIST OFFICE: (b)(6)
(b)(6)

22C OPERATIONS

DEPUTY ASSISTANT DIRECTOR OFFICE: (b)(6)
(b)(6)

DIVISION CHIEF, IRREG/RDA WARFARE OFFICE: (b)(6)
(b)(6)

SUPERVISORY SPECIAL AGENT RDA OFFICE: (b)(6)
(b)(6)

DIVISION CHIEF, OPERATIONS OFFICE: (b)(6)
(b)(6)

26FEB15

SUBJ: NCIS-2 (0022) NATIONAL SECURITY DIRECTORATE KEY PERSONNEL DATA

SUPERVISORY SPECIAL AGENT OPS OFFICE: (b)(6)

(b)(6)

SR. NCIS REP, OUSN, DUSN OFFICE: (b)(6)
(b)(6)

DIVISION CHIEF, SENSITIVE PRO. INTIGRATION OFFICE: (b)(6)
(b)(6)

22D CYBER & DEFENSE CRITICAL INFRASTRUCTURE PROTECTION

DIVISION CHIEF PROGRAMS OFFICE: (b)(6)
(b)(6)

SUPERVISORY SPECIAL AGENT OFFICE: (b)(6)
(b)(6)

CYBER TECH PROGRAM MANAGER OFFICE: (b)(6)
VACANT CELL:

COMPUTER LAW AND NATIONAL SECURITY OFFICE: (b)(6)
(b)(6)

NCIS REP TO CYBERCOM J2X OFFICE: (b)(6)
(b)(6)

NCIS REP TO FCC/C10F OFFICE: (b)(6)
(b)(6)

NCIS REP TO FBI NCIJTF OFFICE: (b)(6)
(b)(6)

22 ANALYTIC DIVISION

SUPERVISORY INTELLIGENCE SPECIALIST OFFICE: (b)(6)
(b)(6)

SUPERVISORY INTELLIGENCE SPECIALIST OFFICE: (b)(6)
(b)(6)

22 LEGAL DIVISION

NATIONAL SECURITY LAW OFFICE: (b)(6)
(b)(6)

2105438 11:11 20151027 IN:SSDEMAIL #4 OUT:NCISWWSSD #3

GENERAL ADMINISTRATION 27OCT15

FROM: 0023 GEN: 23-0037

TO: DIST

SUBJ: NCIS-2 CRIMINAL INVESTIGATIONS DIRECTORATE KEY PERSONNEL DATA SHEET

MAILING ADDRESS
NAVAL CRIMINAL INVESTIGATIVE SERVICE HQ
ATTN: CODE 23
27130 Telegraph Road
Quantico, VA 22134

LOCAL ADDRESS
Same as mailing

TELEPHONES
DSN PREFIX: INCOMING 240-XXXX (LAST 4)
OUTGOING 94-XXX-XXXX (CONUS)
OUTGOING 94-312-XXX-XXXX (OCONUS)
OFFICE:
UNCLASS FAX:
SECURE FAX:

CRIMINAL INVESTIGATIONS DIRECTORATE (0023)

TITLE	PERSONNEL	CONTACT NUMBERS
Executive Assistant Director	(b)(6)	
Assistant Director		
Staff Judge Advocate/ Ethics Counselor		

Admin Officer	(b)(6)

23A - ECONOMIC CRIMES DEPARTMENT

TITLE	PERSONNEL	CONTACT NUMBERS
Deputy Assistant Director 23A1 Div Chief	(b)(6)	

27OCT15

SUBJ: NCIS-2 CRIMINAL INVESTIGATIONS DIRECTORATE KEY PERSONNEL DATA

Economic Crimes	(b)(6)

23B - CRIMINAL INVESTIGATIONS AND OPERATIONS DEPARTMENT

TITLE	PERSONNEL	CONTACT NUMBERS
Deputy Assistant Director	(b)(6)	

TITLE	PERSONNEL	CONTACT NUMBERS

Psychologist	(b)(6)
REACT Cmdr,	
REACT Dep Cmdr	
23B1 Div Chief, DEATH/VIOLENT CRI COLD CASE	
23B2 Div Chief, F&SV/TMU/Insider T	
23B2 SSA, F&SV/TMU/Insider T	
23B3 Div Chief, OPS/Transnational Cr	

23C - PROGRAM MANAGEMENT

TITLE	PERSONNEL	CONTACT NUMBERS
Deputy Assistant Director,	(b)(6)	

27OCT15

SUBJ: NCIS-2 CRIMINAL INVESTIGATIONS DIRECTORATE KEY PERSONNEL DATA

Crim Program Mana	(b)(6)
Senior Representativ to the DODIG	
23C1 Div Chief, Program Manageme	
23C4 Div Chief, Data Analysis	

23D - LAW ENFORCEMENT, PROTECTION, ASSESSMENTS AND SECURITY TRAINING DIVISION

TITLE	PERSONNEL	CONTACT NUMBERS
Deputy Assistan Director LE/Prot Assessment/ Security Trainin	(b)(6)	
23D1Div Chief LE/Protection/A Security Trainin		
23D1 SSA, NJIS/MSA		
23D1 SSA, NJIS/Port Visit S		

DISTRIBUTION
NCISHQ: All Directorates and Departments
INFO: WWSSD

2301811 11:52 20160120 IN:SSDEMAIL #9 OUT:NCISWWSSD #5

GENERAL ADMINISTRATION 20JAN16

FROM: 0025 GEN: 25-0003

TO: DIST

SUBJ: NCIS-2/DIRECTORATE OF INTELLIGENCE AND INFORMATION SHARING
KEY PERSONNEL AND DATA SHEET (0025)

MAILING AND LOCAL ADDRESS
NAVAL CRIMINAL INVESTIGATIVE SERVICE
HEADQUARTERS (NCISHQ CODE 0025)
27130 TELEGRAPH RD
QUANTICO, VA 22134

TELEPHONES
DIIS/MTAC WATCH 571-305-4777/4950
DIIS/MTAC LE DESK 571-305-4900
DSN PREFIX: INCOMING 240-XXXX (LAST 4)
OUTGOING 94-XXX-XXXX (CONUS)
OUTGOING 94-312-XXX-XXXX (OCONUS)
UNCLASS FACSMILIE 571-305-4895
SECURE FACSMILIE (b)(6)

DIRECTORATE OF INTELLIGENCE AND INFORMATION SHARING (0025)

Executive Assistant Director, DIIS

(b)(6)

Assistant Director, DIIS

(b)(6)

SIO/DISL

(b)(6)

Deputy Assistant Director, Operations/
Intelligence Support

(b)(6)

Deputy Assistant Director, Threat Warning and Analysis (ACTING)

(b)(6)

20JAN16

SUBJ: NCIS-2/DIRECTORATE OF INTELLIGENCE AND INFORMATION SHARING KE

(b)(6)

25A - PROGRAM MANAGEMENT, PRODUCTION AND TRAINING

Division Chief, Program Management and Training

(b)(6)

Career Program Manager

(b)(6)

FOSO/Administrative Officer

(b)(6)

(b)(6)

25B - NSD/RDA/CYBER/SCRM TAC

Division Chief, NSD/RDA/CYBER/SCRM TAC

(b)(6)

SIS, RDA / SCRM TAC

(b)(6)

SIS, CYBER

(b)(6)

NATIONAL SECURITY DIRECTORATE

SIS, NSD, CI/RDA

(b)(6)

25C - OPERATIONS SUPPORT

20JAN16

SUBJ: NCIS-2/DIRECTORATE OF INTELLIGENCE AND INFORMATION SHARING KE

Division Chief, Collection & Source Management

(b)(6)

(b)(6)

SIS, Collection & Source Management

(b)(6)

CRIMINAL INVESTIGATIONS DIRECTORATE

Division Chief, Criminal Intelligence Data Analysis

(b)(6)

SIS, Operations & Investigations Support

(b)(6)

25D - THREAT WARNING & ANALYSIS

Division Chief - Biometrics/D-DEx/LInX,
Biometrics and eGuardian

(b)(6)

Division Chief, MTAC Current Intelligence/ Americas

(b)(6)

SIS, Americas
VACANT

Division Chief, Pacific

(b)(6)

SIS, Pacific

(b)(6)

Division Chief, Europe/Africa & Middle East

20JAN16

SUBJ: NCIS-2/DIRECTORATE OF INTELLIGENCE AND INFORMATION SHARING KE

(b)(6)

SIS, Europe/Africa Division

(b)(6)

SIS, Middle East

(b)(6)

Division Chief, Production

(b)(6)

DIIS SUPPORT TO FIELD COMPONENTS

GLOBAL OPERATIONS

SIO, EADGLOBAL

(b)(6)

SIS, EADGLOBAL

(b)(6)

SIS, CBFO

(b)(6)

ATLANTIC OPERATIONS

SIO, EADLANT

(b)(6)

SIO, Europe/Africa Field Office

(b)(6)

20JAN16

SUBJ: NCIS-2/DIRECTORATE OF INTELLIGENCE AND INFORMATION SHARING KE

(b)(6)

SIO, Northeast Field Office

(b)(6)

SIO, Southeast Field Office

(b)(6)

SIO, Norfolk Field Office

(b)(6)

SIO, Washington Field Office

(b)(6)

SIO, Middle East Field Office

(b)(6)

PACIFIC OPERATIONS

SIO, EADPAC

(b)(6)

SIO, Singapore Field Office

(b)(6)

SIO, Far East Field Office

(b)(6)

20JAN16

SUBJ: NCIS-2/DIRECTORATE OF INTELLIGENCE AND INFORMATION SHARING KE

SIO, Northwest Field Office

(b)(6)

SIO, Hawaii Field Office

(b)(6)

SIO, Southwest Field Office

(b)(6)

IS, Marine West Field Office

(b)(6)

25X- GLOBAL ENGAGEMENT

Division Chief, Engagement

(b)(6)

GENERAL ADMINISTRATION 12FEB16

FROM: 2AZL GEN: ZL-0003

TO: DIST

SUBJ: NCIS-2/(2AZV) STAAT LANT VA BEACH DETACHMENT DATA SHEET

MAILING ADDRESS LOCAL ADDRESS
1430 HELICOPTER RD STE 250 BLDG 3801 JEB LITTLE CREEK-FORT STORY
VA BEACH, VA 23459 1430 HELICOPTER RD STE 250
VA BEACH, VA 23459

TELEPHONES COMMERCIAL DSN
OFFICE (757) 462-8925/7893 (312)253-8925/7893
UNCLAS FAX (757) 462-4997

MSG PLA: NAVCRIMINVSERV STAAT NORFOLK VA OFFICE CODE: 2AZV
UIC: 63055

TERRIORIAL COVERAGE:
CONNECTICUT, ILLINOIS, INDIANA, KENTUCKY, MAINE, MASSACHUSETTS, MICHIGAN, NEW HAMPSHIRE, NEW JERSEY, NEW YORK, OHIO, PENNSYLVANIA, RHODE ISLAND, VERMOUNT, AND WISCONSIN.
EASTERN CANADA TO INCLUDE: PROVINCES OF ONTARIO, QUEBEC, NEW BRUNSWICK, NEWFOUNDLAND, NOVA SCOTIA AND PRINCE EDWARD ISLAND.
DISTRICT OF COLUMBIA: ALL AREAS
MARYLAND COUNTIES: ALLEGANY, CHARLES, FREDERICK, GARRETT, PRINCE GEORGE'S, WASHINGTON
VIRGINIA COUNTIES: ARLINGTON, CAROLINE, CLARKE, CULPEPPER, ESSEX, FAIRFAX, FAUQUIER, FREDERICK, GREENE, KING GEORGE, LANCASTER, LOUDOUN, MADISON, NORTHCUMBERLAND, ORANGE, PAGE, PRINCE WILLIAM, RAPPAHANNOCK, RICHMOND, ROCKINGHAM, SHENANDOAH, SPOTSYLVANIA, STAFFORD, WARREN, WESTMORELAND.
WEST VIRGINIA COUNTIES: BARBOUR, BERKELEY, DODD RIDGE, GRANT, HAMPSHIRE, HARDY, HARRISON, JEFFERSON, MARION, MINERAL, MONONGALIA, MORGAN, PLEASANTS, PRESTON, RITCHIE, TAYLOR, TUCKER, TYLER, WETZEL, WOOD.

DISTRIBUTION
INFO: WWSSD

FOR OFFICIAL USE ONLY
PAGE 1 LAST (b)(6)

2301709 11:33 20160120 IN:SSDEMAIL #7 OUT:NCISWWSSD #4

GENERAL ADMINISTRATION 15JAN16

FROM: 2GJQ GEN: 02G-0001

TO: DIST

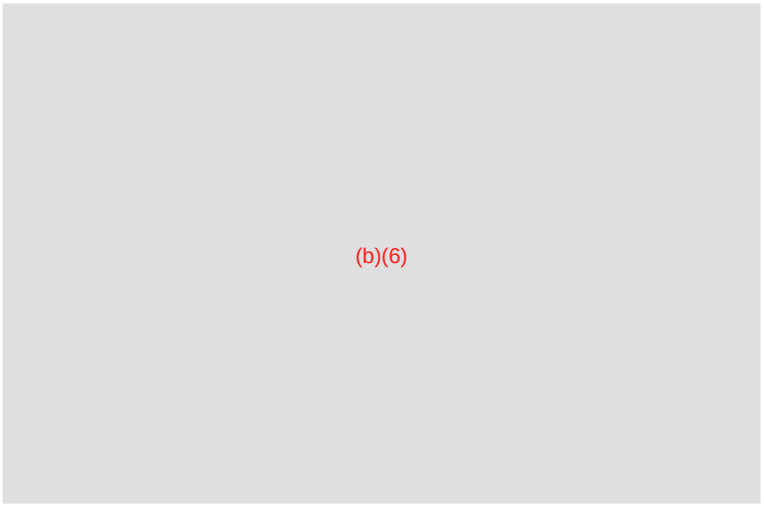
SUBJ: NCIS-2: COUNTERINTELLIGENCE TECHNICAL SERVICES KEY PERSONNEL
DATA SHEET

MAILING ADDRESS:
NAVAL CRIMINAL INVESTIGATIVE SERVICE HEADQUARTERS CODE 2GJQ RUSSELL KNOX BUILDING
27130 TELEGRAPH ROAD
QUANTICO VA 22134-2253

ALL EMAILS SHOULD BE ADDRESSED TO: (b)(6)
STE: b7E

TITLE CONTACT INFORMATION

(b)(6)



15JAN16

SUBJ: NCIS-2: COUNTERINTELLIGENCE TECHNICAL SERVICES KEY PERSONNEL D

(b)(6)

HAWAII
MAILING ADDRESS:
NCIS HAWAII
ATTN Code 2GJV
449 SOUTH AVE
PEARL HARBOR HI 96860

(b)(6)

NORFOLK
MAILING ADDRESS:
NCIS OCEANA
ATTN CODE 2GJT
1801 TOMCAT BLVD

VIRGINIA BEACH VA 23460

(b)(6)

SAN DIEGO
MAILING ADDRESS:
NCIS SAN DIEGO
ATTN CODE 2GJU
3405 WELLES ST STE 1
SAN DIEGO CA 92136

(b)(6)

ALL DISCUSSIONS OF PENDING TSCM REQUESTS, SCHEDULING AND INVESTIGATIVE PROCEDURES ARE CLASSIFIED MINIMUM SECRET/NOFORN PER DODINST 5240.05

2202722 17:23 20151208 IN:SSDEMAIL #3 OUT:NCISWWSSD #1

GENERAL ADMINISTRATION 08DEC15

FROM: 2PZP GEN: ZP-0003

TO: DIST

SUBJ: NCIS-2: (2PZP) NCIS SECURITY TRAINING, ASSISTANCE, ASSESSMENT
TEAM PACIFIC FIELD OFFICE KEY PERSONNEL

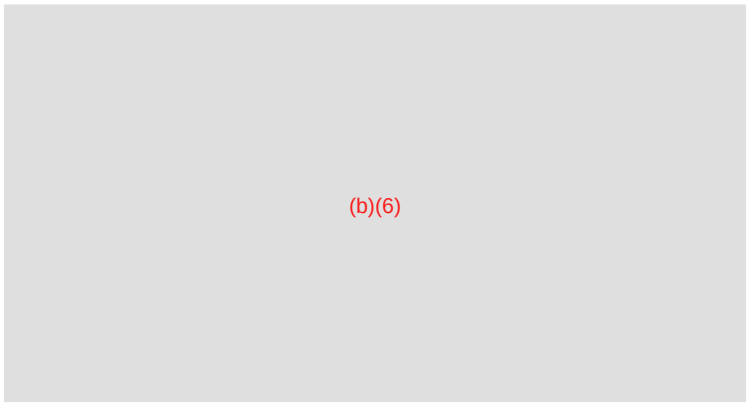
MAILING ADDRESS LOCAL ADDRESS
SECURITY SPECIALIST IN CHARGE (b)(6)
PO BOX 357053 (b)(6)
SAN DIEGO CA 92135-7053 (b)(6)

TELEPHONES: COMMERCIAL: (CONUS 011) DSN: 312
OFFICE (619) 545-9427/8934 735/577
AFTER HOURS (619) 204-1116(LCDR (b)(6)
OPERATIONS OFFICER)
UNCLAS FACSIMILE (619) 545-6166 735-6166
STE b7E

STAAT PAC PERSONNEL (UIC) 63057

SECURITY SPECIALIST IN CHARGE

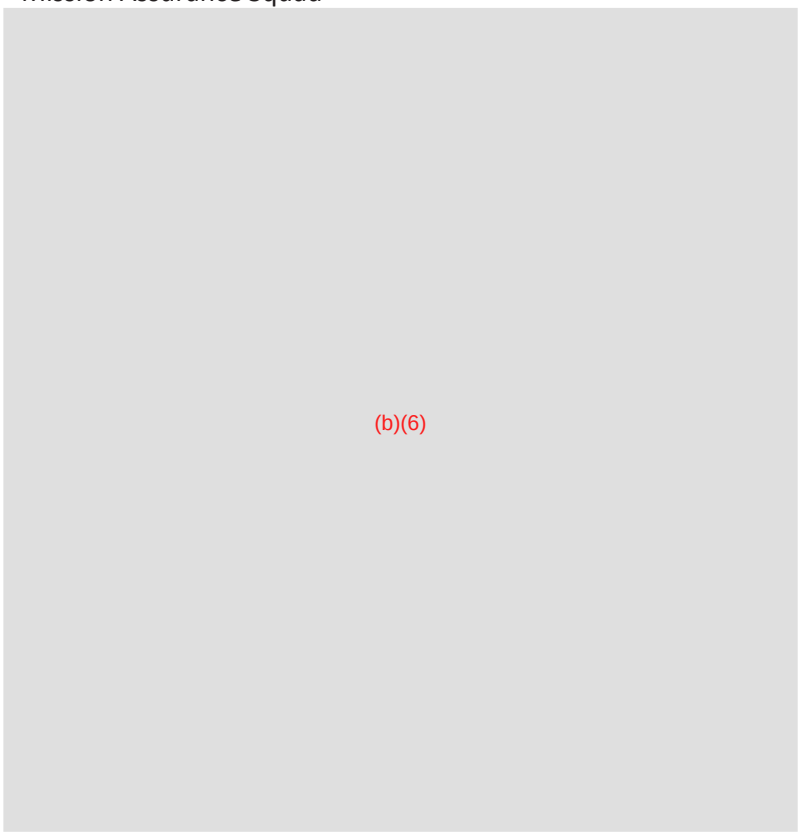
(b)(6)



08DEC15

SUBJ: NCIS-2: (2PZP) NCIS SECURITY TRAINING, ASSISTANCE, ASSESSMENT

Mission Assurance Squad



(b)(6)

STAAT PAC SINGAPORE DETACHMENT (UIC) 40484 DSN: (b)(6)

(b)(6)

STAAT PAC YOKOSUKA DETACHMENT (UIC) 0765A DSN: (b)(6)

(b)(6)

STAAT PAC MANILA UNIT

(b)(6)

DMS: PLA: NAVCRIMINVSERV STAAT SAN DIEGO CA//2PZP//

SSD ELECTRICAL DISTRIBUTION CODE: /2PZP//

SUBORDINATE OFFICES:

STAAT PAC NORTHWEST DETACHMENT (2PZA)
STAAT PAC SINGAPORE DETACHMENT (2PZS)
STAAT PAC MANILA UNIT (2PZI)

08DEC15

SUBJ: NCIS-2: (2PZP) NCIS SECURITY TRAINING, ASSISTANCE, ASSESSMENT

STAAT PAC FAR EAST DETACHMENT (2PZY)

TERRITORIAL COVERAGE:

THE GEOGRAPHICAL AREA OF RESPONSIBILITY OF NCIS STAAT PAC INCLUDES AREAS ASSIGNED TO NCIS SOUTHWEST FIELD OFFICE, NORTHWEST FIELD OFFICE, SINGAPORE FIELD OFFICE, FAR EAST FIELD OFFICE, HAWAII FIELD OFFICE, AND MARINE CORPS WEST FIELD OFFICE.

ADDRESSES FOR STAAT PAC OFFICES:

NCIS STAAT SAN DIEGO FIELD OFFICE
P O BOX 350753
SAN DIEGO CA 92135-7053

OR

(b)(6)

NCIS FAR EAST FIELD OFFICE
ATTN SSS (b)(6)
PSC 473 BOX 76
FPO AP 96349-0076

OR

NCIS STAAT FAR EAST OFFICE

(b)(6)

OR FOR FED EX

NCIS FAR EAST FIELD OFFICE

(b)(6)

NCIS SINGAPORE OFFICE

(b)(6)

08DEC15

SUBJ: NCIS-2: (2PZP) NCIS SECURITY TRAINING, ASSISTANCE, ASSESSMENT

OR

FLEET LOGISTIC CENTER YOKOSUKA
SITE SINGAPORE
PSA SEMBAWANG TERMINAL
DEPTFORD ROAD BLDG-7-4
SINGAPORE 759657
M/F: (b)(6)

NCISRA MANILA OFFICE

(b)(6)

OR
CHANCERY BUILDING
AMERICAN EMBASSY MANILA
1201 ROXAS BLVD., ERMITA
MANILA, 1000, PHILIPPINES

DISTRIBUTION:
//WWSSD//

FOR OFFICIAL USE ONLY
PAGE 4 LAST (b)(6)

21AUG09

NCIS-2: (0021) COMBATING TERRORISM DIRECTORATE KEY PERSONNEL DATA SHEET

MAILING ADDRESS
NAVAL CRIMINAL INVESTIGATIVE SERVICE
HEADQUARTERS (NCISHQ CODE 0021)
716 SICARD ST., SE, SUITE 2000
WASHINGTON NAVY YARD, BLDG 111
WASHINGTON, DC 20388-5380

TELEPHONES
DSN PREFIX: 288/325 FOR 685 NUMBERS
OFFICE: 202-433-9077
UNCLASS FAX: 202-433-9147
CLASS FAX: (b)(6)

CODE/PERSONNEL	TELEPHONE NUMBERS
21 COMBATING TERRORISM DIRECTORATE	
EXECUTIVE ASSISTANT DIRECTOR (b)(6)	OFFICE: CELL:
21A PROGRAM DIRECTION DEPARTMENT	
DEPUTY ASSISTANT DIRECTOR (b)(6)	OFFICE: CELL: HOME:
DIVISION CHIEF (b)(6)	OFFICE: CELL: HOME:
SUPERVISORY SPECIAL AGENT (b)(6)	OFFICE: CELL:
STATE DEPT REPRESENTATIVE (b)(6)	OFFICE: CELL: HOME:
BUDGET/TRAVEL VACANT TEMP POC b6	OFFICE: CELL:
LEAD INVESTIGATIONS REVIEW SPECIALIST (b)(6)	OFFICE: CELL:
21A1 PHYSICAL SECURITY/ANTI-TERRORISM DIVISION	
DIVISION CHIEF (b)(6)	OFFICE: CELL:
STAAT TRAINING PROGRAM MANAGER VACANT	OFFICE: CELL: HOME

(b)(6)

STAAT CNOIVA PROGRAM MANAGER
(b)(6)
OFFICE:
CELL:
HOME:

STAAT MSC-ISA PROGRAM MANAGER
(b)(6)
OFFICE:
CELL:
HOME:

STAAT PIVA PROGRAM MANAGER
(b)(6)
OFFICE:
CELL:
HOME:

DESK OFFICER (FPD MATTERS)
(b)(6)
OFFICE:
CELL:
HOME:

21B CT OPERATIONS AND INVESTIGATIONS DEPARTMENT

DEPUTY ASSISTANT DIRECTOR
(b)(6)
OFFICE:
CELL:
HOME:

NJTTF DEPUTY UNIT CHIEF
TBD
OFFICE: TBD
CELL: TBD
HOME: TBD

DIVISION CHIEF, SENIOR REP - FBIHQ, CTD
INTERNATIONAL TERRORISM OPERATIONS SECTION
(b)(6)
OFFICE:
CELL:
HOME:

OARDEC REPRESENTATIVE
(b)(6)
OFFICE:
CELL:
HOME:

21B PACIFIC DIVISION

DIVISION CHIEF
(b)(6)
OFFICE:
CELL:

LNO SPECIAL OPERATIONS COMMAND (SOCOM)
(b)(6)
OFFICE:
HOME:

LNO CENTRAL COMMAND (CENTCOM)
(b)(6)
OFFICE:
CELL:

21B ATLANTIC DIVISION

DIVISION CHIEF
(b)(6)
OFFICE:
CELL:
HOME:

SUPERVISORY SPECIAL AGENT OPS/INV
(b)(6)
OFFICE:
CELL: TBD

(b)(6)

(b)(6)

CT ANALYTICAL DIVISION CHIEF
(b)(6)
OFFICE:
CELL:
HOME:

21B1 PROTECTIVE OPERATIONS DEPARTMENT

DEPUTY ASSISTANT DIRECTOR
(b)(6)
OFFICE:
CELL:
HOME:

PERSONAL SECURITY ADVISOR CMC
(b)(6)
OFFICE:
CELL:
HOME:

PERSONAL SECURITY ADVISOR CNO
(b)(6)
OFFICE:
CELL:

PERSONAL SECURITY ADVISOR SECNAV
(b)(6)
OFFICE:
CELL:
HOME:

PERSONAL SECURITY ADVISOR CJCS
(b)(6)
OFFICE:
CELL:
HOME:

OPERATIONS OFFICER
(b)(6)
OFFICE:
CELL:
HOME:

SSA PROTECTIVE SERVICE OPERATIONS
(b)(6)
OFFICE:
CELL:
HOME:

(b)(6)

21B CRIMINAL INVESTIGATIVE TASK FORCE (CITF) FT. BELVOIR

SPECIAL AGENT IN CHARGE
(b)(6)
OFFICE:
CELL:

ASSISTANT SPECIAL AGENT IN CHARGE
(b)(6)
OFFICE:
CELL:
HOME:

SUPERVISORY SPECIAL AGENT
(b)(6)
OFFICE:
CELL:
HOME:

(b)(6)

1457013 10:49 20150226 IN:SSDEMAIL #2 OUT:NCISWWSSD #2

GENERAL ADMINISTRATION 26FEB15

FROM: 0022 GEN: 22-0003

TO: DIST

SUBJ: NCIS-2 (0022) NATIONAL SECURITY DIRECTORATE KEY PERSONNEL DATA SHEET

MAILING ADDRESS
NAVAL CRIMINAL INVESTIGATIVE SERVICE
HEADQUARTERS (NCISHQ CODE 0022)
27130 TELEGRAPH ROAD
QUANTICO, VA 22134

TELEPHONES
DSN PREFIX: INCOMING 240-XXXX (LAST 4)
OUTGOING 94-XXX-XXXX (CONUS)
OUTGOING 94-312-XXX-XXXX (OCONUS)
OFFICE: 571-305-9689 (TEMP)
UNCLASS FAX: 571-305-9574
SECURE FAX: (b)(6)

NAVMSG PLA: NAVCRIMINVSERVHQ NSD QUANTICO VA

CODE/PERSONNEL TELEPHONE NUMBERS

EXECUTIVE ASSISTANT DIRECTORATE OFFICE: (b)(6)
(b)(6)

ASSISTANT DIRECTOR OFFICE: (b)(6)
(b)(6)

SENIOR POLICY ADVISOR OFFICE: (b)(6)
(b)(6)

STATE DEPARTMENT REPRESENTATIVE OFFICE: (b)(6)
(b)(6)

DEPUTY UNDER SECRETARY DEFENSE INTEL OFFICE: (b)(6)
(b)(6)

JOINT STAFF CCICA OFFICE: (b)(6)
(b)(6)

22A PROGRAM DIRECTION

DEPUTY ASSISTANT DIRECTOR OFFICE: (b)(6)
(b)(6)

SENIOR PROGRAM ANALYST OFFICE: (b)(6)
(b)(6)

FOR OFFICIAL USE ONLY
PAGE 1

26FEB15

SUBJ: NCIS-2 (0022) NATIONAL SECURITY DIRECTORATE KEY PERSONNEL DATA

DIVISION CHIEF OFFICE: (b)(6)
(b)(6)

SUPERVISORY SPECIAL AGENT PROGRAMS/POLICY OFFICE: (b)(6)
(b)(6)

FPD PROGRAM MANAGER OFFICE: (b)(6)
(b)(6)

FOSO OFFICE: (b)(6)
(b)(6)

22B INVESTIGATIONS

DEPUTY ASSISTANT DIRECTOR OFFICE: (b)(6)
(b)(6)

DIVISION CHIEF OFFICE: (b)(6)
(b)(6)

SUPERVISORY SPECIAL AGENT INV OFFICE: (b)(6)
(b)(6)

DIVISION CHIEF INSIDER THREAT OFFICE: (b)(6)
(b)(6)

SUPERVISORY SPECIAL AGENT INSIDER THREAT OFFICE: (b)(6)
(b)(6)

LNO N2N6 OFFICE: (b)(6)
(b)(6)

NJTTF DEPUTY UNIT CHIEF OFFICE: (b)(6)
(b)(6)

STAFF PSYCHOLOGIST OFFICE: (b)(6)
(b)(6)

22C OPERATIONS

DEPUTY ASSISTANT DIRECTOR OFFICE: (b)(6)
(b)(6)

DIVISION CHIEF, IRREG/RDA WARFARE OFFICE: (b)(6)
(b)(6)

SUPERVISORY SPECIAL AGENT RDA OFFICE: (b)(6)
(b)(6)

DIVISION CHIEF, OPERATIONS OFFICE: (b)(6)
(b)(6)

26FEB15

SUBJ: NCIS-2 (0022) NATIONAL SECURITY DIRECTORATE KEY PERSONNEL DATA

SUPERVISORY SPECIAL AGENT OPS OFFICE: (b)(6)

(b)(6)

SR. NCIS REP, OUSN, DUSN OFFICE: (b)(6)
(b)(6)

DIVISION CHIEF, SENSITIVE PRO. INTIGRATION OFFICE: (b)(6)
(b)(6)

22D CYBER & DEFENSE CRITICAL INFRASTRUCTURE PROTECTION

DIVISION CHIEF PROGRAMS OFFICE: (b)(6)
(b)(6)

SUPERVISORY SPECIAL AGENT OFFICE: (b)(6)
(b)(6)

CYBER TECH PROGRAM MANAGER OFFICE: (b)(6)
VACANT CELL:

COMPUTER LAW AND NATIONAL SECURITY OFFICE: (b)(6)
(b)(6)

NCIS REP TO CYBERCOM J2X OFFICE: (b)(6)
(b)(6)

NCIS REP TO FCC/C10F OFFICE: (b)(6)
(b)(6)

NCIS REP TO FBI NCIJTF OFFICE: (b)(6)
(b)(6)

22 ANALYTIC DIVISION

SUPERVISORY INTELLIGENCE SPECIALIST OFFICE: (b)(6)
(b)(6)

SUPERVISORY INTELLIGENCE SPECIALIST OFFICE: (b)(6)
(b)(6)

22 LEGAL DIVISION

NATIONAL SECURITY LAW OFFICE: (b)(6)
(b)(6)

2105438 11:11 20151027 IN:SSDEMAIL #4 OUT:NCISWWSSD #3

GENERAL ADMINISTRATION 27OCT15

FROM: 0023 GEN: 23-0037

TO: DIST

SUBJ: NCIS-2 CRIMINAL INVESTIGATIONS DIRECTORATE KEY PERSONNEL DATA SHEET

MAILING ADDRESS
NAVAL CRIMINAL INVESTIGATIVE SERVICE HQ
ATTN: CODE 23
27130 Telegraph Road
Quantico, VA 22134

LOCAL ADDRESS
Same as mailing

TELEPHONES
DSN PREFIX: INCOMING 240-XXXX (LAST 4)
OUTGOING 94-XXX-XXXX (CONUS)
OUTGOING 94-312-XXX-XXXX (OCONUS)
OFFICE:
UNCLASS FAX:
SECURE FAX:

CRIMINAL INVESTIGATIONS DIRECTORATE (0023)

TITLE	PERSONNEL	CONTACT NUMBERS
Executive Assistant Director	(b)(6)	
Assistant Director		
Staff Judge Advocate/ Ethics Counselor		

Admin Officer	(b)(6)

23A - ECONOMIC CRIMES DEPARTMENT

TITLE	PERSONNEL	CONTACT NUMBERS
Deputy Assistant Director 23A1 Div Chief	(b)(6)	

27OCT15

SUBJ: NCIS-2 CRIMINAL INVESTIGATIONS DIRECTORATE KEY PERSONNEL DATA

Economic Crimes	(b)(6)

23B - CRIMINAL INVESTIGATIONS AND OPERATIONS DEPARTMENT

TITLE	PERSONNEL	CONTACT NUMBERS
Deputy Assistant Director	(b)(6)	

TITLE	PERSONNEL	CONTACT NUMBERS

Psychologist	(b)(6)
REACT Cmdr,	
REACT Dep Cmdr	
23B1 Div Chief, DEATH/VIOLENT CRI COLD CASE	
23B2 Div Chief, F&SV/TMU/Insider T	
23B2 SSA, F&SV/TMU/Insider T	
23B3 Div Chief, OPS/Transnational Cr	

23C - PROGRAM MANAGEMENT

TITLE	PERSONNEL	CONTACT NUMBERS
Deputy Assistant Director,	(b)(6)	

27OCT15

SUBJ: NCIS-2 CRIMINAL INVESTIGATIONS DIRECTORATE KEY PERSONNEL DATA

Crim Program Mana	(b)(6)
Senior Representativ to the DODIG	
23C1 Div Chief, Program Manageme	
23C4 Div Chief, Data Analysis	

23D - LAW ENFORCEMENT, PROTECTION, ASSESSMENTS AND SECURITY TRAINING DIVISION

TITLE	PERSONNEL	CONTACT NUMBERS
Deputy Assistan Director LE/Prot Assessment/ Security Trainin	(b)(6)	
23D1Div Chief LE/Protection/A Security Trainin		
23D1 SSA, NJIS/MSA		
23D1 SSA, NJIS/Port Visit S		

DISTRIBUTION
NCISHQ: All Directorates and Departments
INFO: WWSSD

2301811 11:52 20160120 IN:SSDEMAIL #9 OUT:NCISWWSSD #5

GENERAL ADMINISTRATION 20JAN16

FROM: 0025 GEN: 25-0003

TO: DIST

SUBJ: NCIS-2/DIRECTORATE OF INTELLIGENCE AND INFORMATION SHARING
KEY PERSONNEL AND DATA SHEET (0025)

MAILING AND LOCAL ADDRESS
NAVAL CRIMINAL INVESTIGATIVE SERVICE
HEADQUARTERS (NCISHQ CODE 0025)
27130 TELEGRAPH RD
QUANTICO, VA 22134

TELEPHONES
DIIS/MTAC WATCH 571-305-4777/4950
DIIS/MTAC LE DESK 571-305-4900
DSN PREFIX: INCOMING 240-XXXX (LAST 4)
OUTGOING 94-XXX-XXXX (CONUS)
OUTGOING 94-312-XXX-XXXX (OCONUS)
UNCLASS FACSMILIE 571-305-4895
SECURE FACSMILIE (b)(6)

DIRECTORATE OF INTELLIGENCE AND INFORMATION SHARING (0025)

Executive Assistant Director, DIIS

(b)(6)

Assistant Director, DIIS

(b)(6)

SIO/DISL

(b)(6)

Deputy Assistant Director, Operations/
Intelligence Support

(b)(6)

Deputy Assistant Director, Threat Warning and Analysis (ACTING)

(b)(6)

20JAN16

SUBJ: NCIS-2/DIRECTORATE OF INTELLIGENCE AND INFORMATION SHARING KE

(b)(6)

25A - PROGRAM MANAGEMENT, PRODUCTION AND TRAINING

Division Chief, Program Management and Training

(b)(6)

Career Program Manager

(b)(6)

FOSO/Administrative Officer

(b)(6)

(b)(6)

25B - NSD/RDA/CYBER/SCRM TAC

Division Chief, NSD/RDA/CYBER/SCRM TAC

(b)(6)

SIS, RDA / SCRM TAC

(b)(6)

SIS, CYBER

(b)(6)

NATIONAL SECURITY DIRECTORATE

SIS, NSD, CI/RDA

(b)(6)

25C - OPERATIONS SUPPORT

20JAN16

SUBJ: NCIS-2/DIRECTORATE OF INTELLIGENCE AND INFORMATION SHARING KE

Division Chief, Collection & Source Management

(b)(6)

(b)(6)

SIS, Collection & Source Management

(b)(6)

CRIMINAL INVESTIGATIONS DIRECTORATE

Division Chief, Criminal Intelligence Data Analysis

(b)(6)

SIS, Operations & Investigations Support

(b)(6)

25D - THREAT WARNING & ANALYSIS

Division Chief - Biometrics/D-DEx/LInX,
Biometrics and eGuardian

(b)(6)

Division Chief, MTAC Current Intelligence/ Americas

(b)(6)

SIS, Americas
VACANT

Division Chief, Pacific

(b)(6)

SIS, Pacific

(b)(6)

Division Chief, Europe/Africa & Middle East

20JAN16

SUBJ: NCIS-2/DIRECTORATE OF INTELLIGENCE AND INFORMATION SHARING KE

(b)(6)

SIS, Europe/Africa Division

(b)(6)

SIS, Middle East

(b)(6)

Division Chief, Production

(b)(6)

DIIS SUPPORT TO FIELD COMPONENTS

GLOBAL OPERATIONS

SIO, EADGLOBAL

(b)(6)

SIS, EADGLOBAL

(b)(6)

SIS, CBFO

(b)(6)

ATLANTIC OPERATIONS

SIO, EADLANT

(b)(6)

SIO, Europe/Africa Field Office

(b)(6)

20JAN16

SUBJ: NCIS-2/DIRECTORATE OF INTELLIGENCE AND INFORMATION SHARING KE

(b)(6)

SIO, Northeast Field Office

(b)(6)

SIO, Southeast Field Office

(b)(6)

SIO, Norfolk Field Office

(b)(6)

SIO, Washington Field Office

(b)(6)

SIO, Middle East Field Office

(b)(6)

PACIFIC OPERATIONS

SIO, EADPAC

(b)(6)

SIO, Singapore Field Office

(b)(6)

SIO, Far East Field Office

(b)(6)

20JAN16

SUBJ: NCIS-2/DIRECTORATE OF INTELLIGENCE AND INFORMATION SHARING KE

SIO, Northwest Field Office

(b)(6)

SIO, Hawaii Field Office

(b)(6)

SIO, Southwest Field Office

(b)(6)

IS, Marine West Field Office

(b)(6)

25X- GLOBAL ENGAGEMENT

Division Chief, Engagement

(b)(6)

1971693 12:52 20150904 IN:SSDEMAIL #1 OUT:NCISWWSSD #1

GENERAL ADMINISTRATION 04SEP15

FROM: CALE GEN: LE-0014

TO: DIST

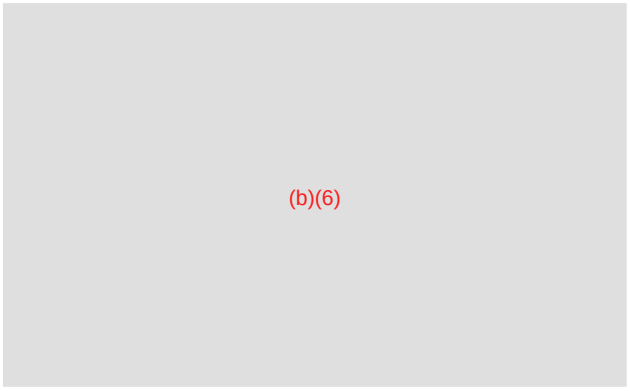
SUBJ: CAFO KEY PERSONNEL LISTING

MAILING ADDRESS:
SPECIAL AGENT IN CHARGE
NAVAL CRIMINAL INVESTIGATIVE SERVICE
Bldg. H-32 JULIAN C. SMITH DRIVE
CAMP LEJEUNE NC 28547

DMS PLA: NAVCRIMINVSERVFO CAROLINAS CAMP LEJEUNE NC

TELEPHONES: COMMERCIAL: (910) 451-8600 DSN: 751-8600 UNCLASS FAX: (910) 451-8206

(b)(6)

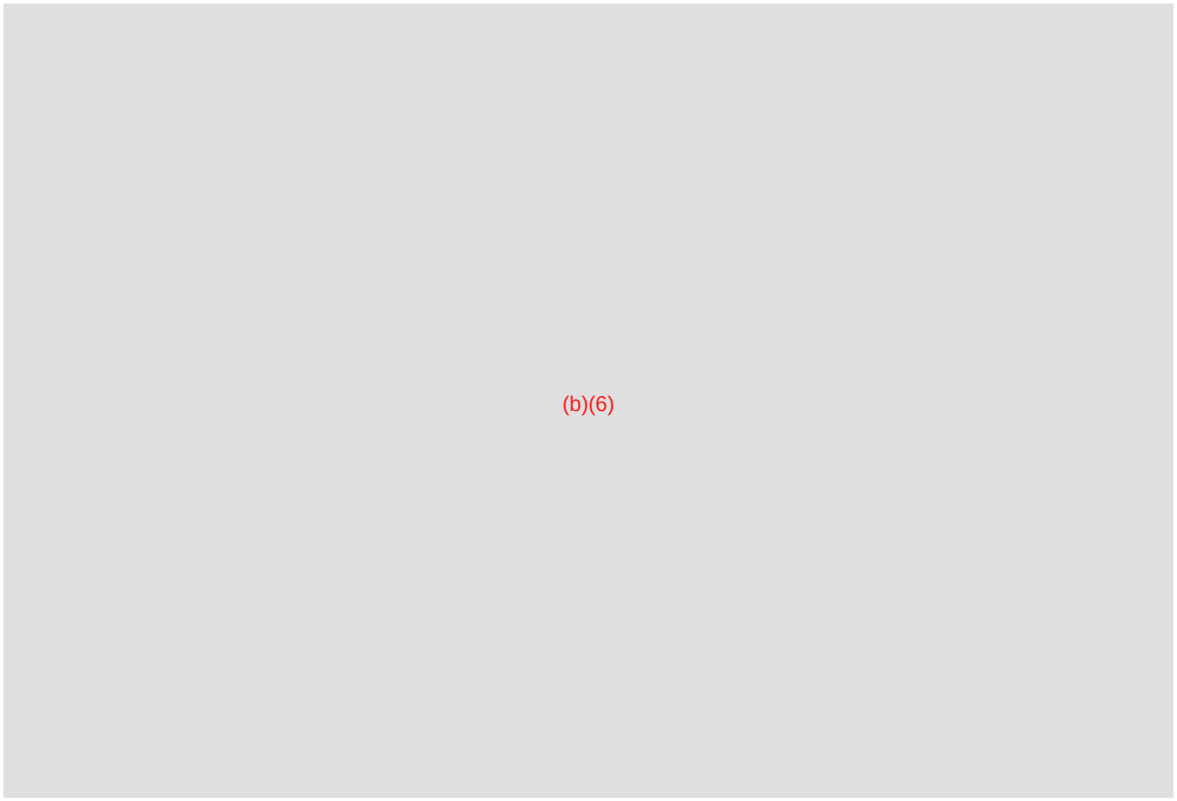


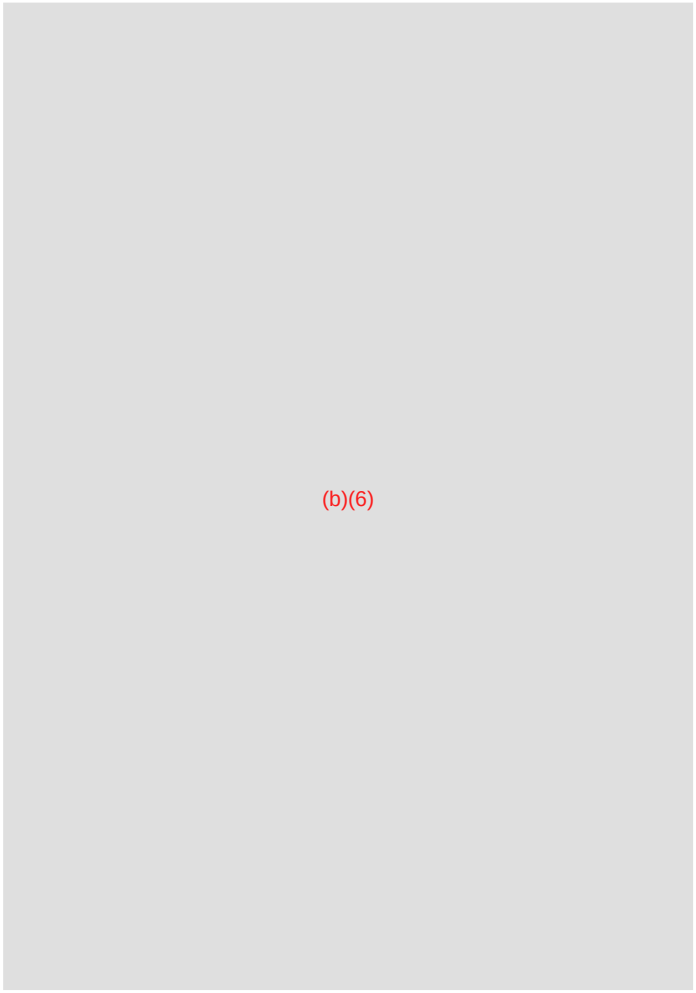
SUPERVISORY SPECIAL AGENT - FAMILY AND SEXUAL VIOLENCE (CHILD) (b)(6)

FOR OFFICIAL USE ONLY
PAGE 1

04SEP15

SUBJ: CAFO KEY PERSONNEL LISTING



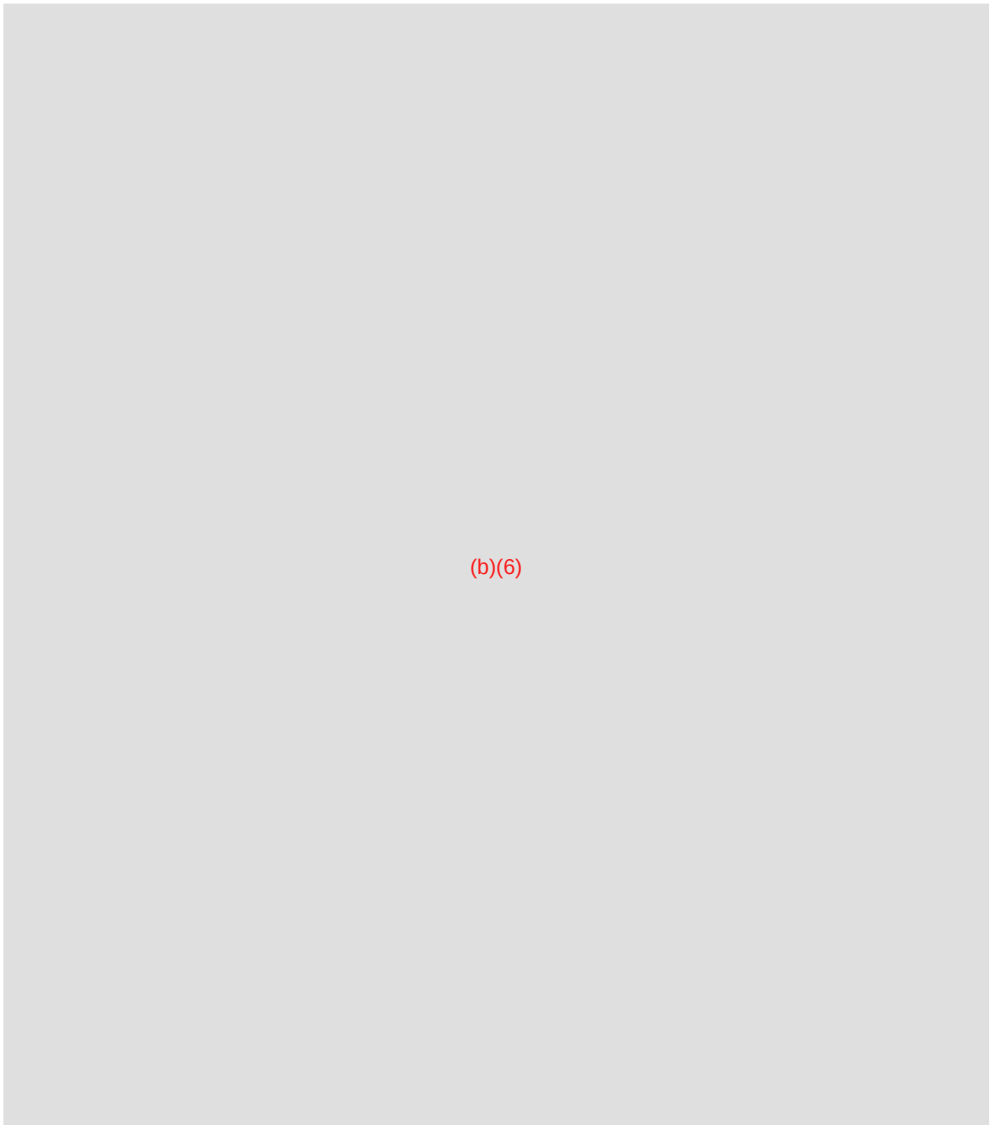


04SEP15

SUBJ: CAFO KEY PERSONNEL LISTING

FIELD COMPUTER SPECIALIST - VACANT
OFFICE: (b)(6)
MOBILE:
RESIDENCE:

INVESTIGATIVE SPECIALIST (CI/CT)



DISTRIBUTION:
INFO: ALL NCIS FO & HQ DIRECTORATE

1832795 15:38 20150717 IN:SSDEMAIL #7 OUT:NCISWWSSD #3

GENERAL ADMINISTRATION 17JUL15

FROM: CALE GEN: LE-0010

TO: DIST

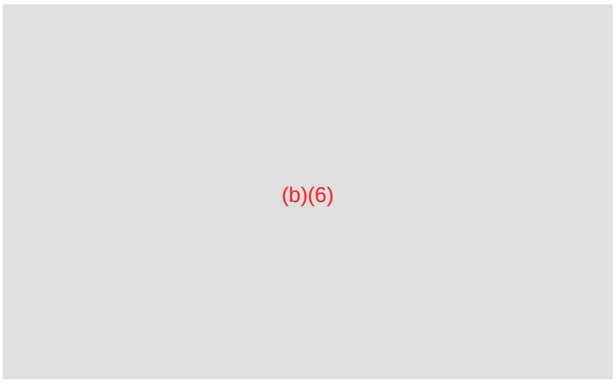
SUBJ: CAFO KEY PERSONNEL LISTING **CORRECTED COPY**

MAILING ADDRESS:
SPECIAL AGENT IN CHARGE
NAVAL CRIMINAL INVESTIGATIVE SERVICE
H 32 JULIAN C SMITH DRIVE
CAMP LEJEUNE NC 28547

DMS PLA: NAVCRIMINVSERVFO CAROLINAS CAMP LEJEUNE NC

TELEPHONES: COMMERCIAL: (910) 451-8600 DSN: 751-8600 UNCLASS FAX: (910) 451-8206

(b)(6)

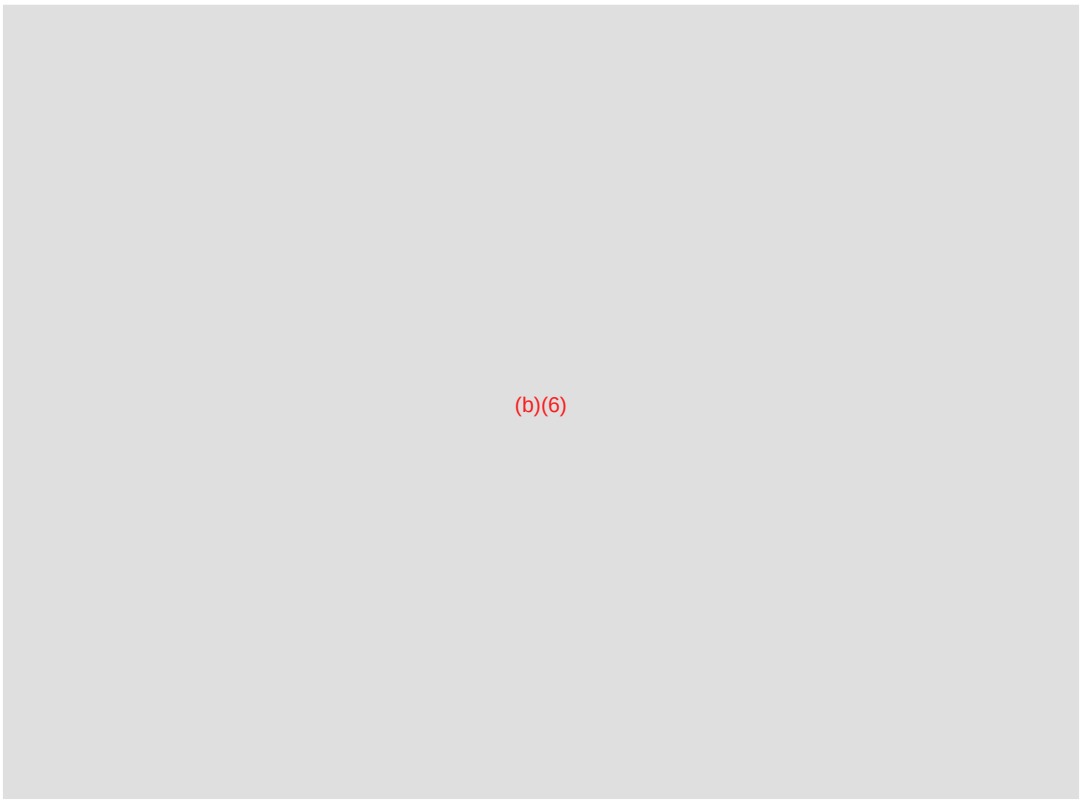


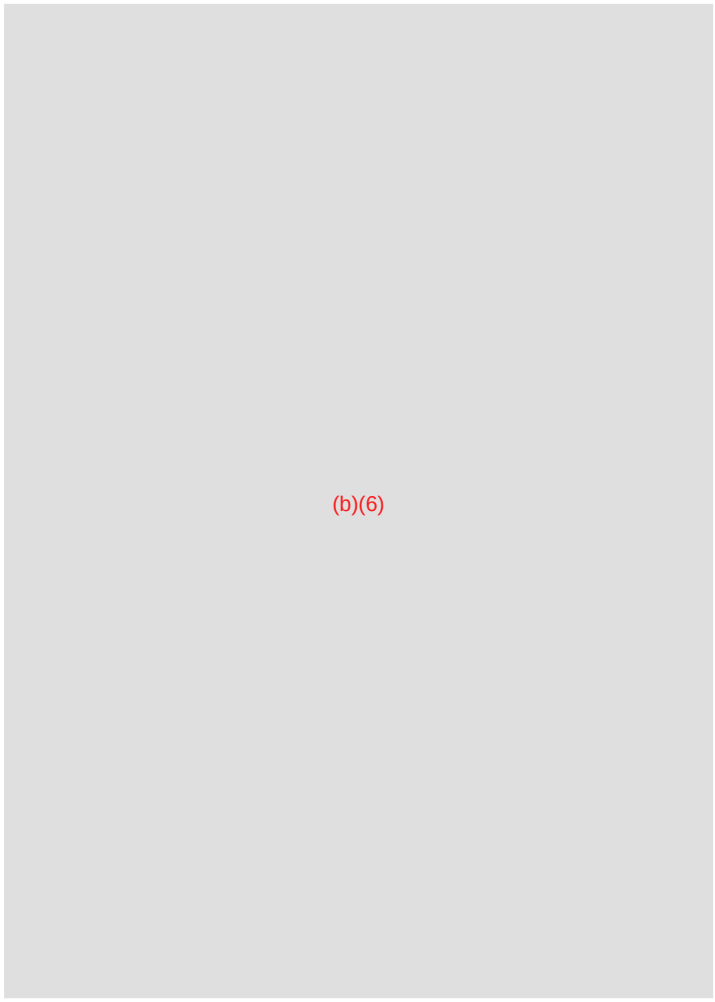
SUPERVISORY SPECIAL AGENT - FAMILY AND SEXUAL VIOLENCE (b)(6)

FOR OFFICIAL USE ONLY
PAGE 1

17JUL15

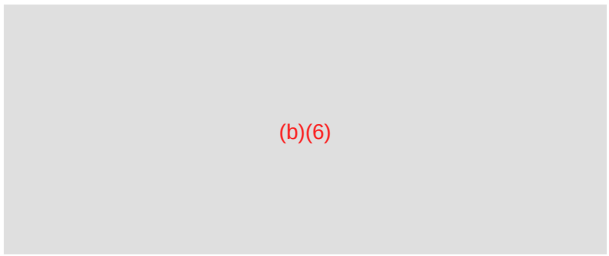
SUBJ: CAFO KEY PERSONNEL LISTING **CORRECTED COPY**

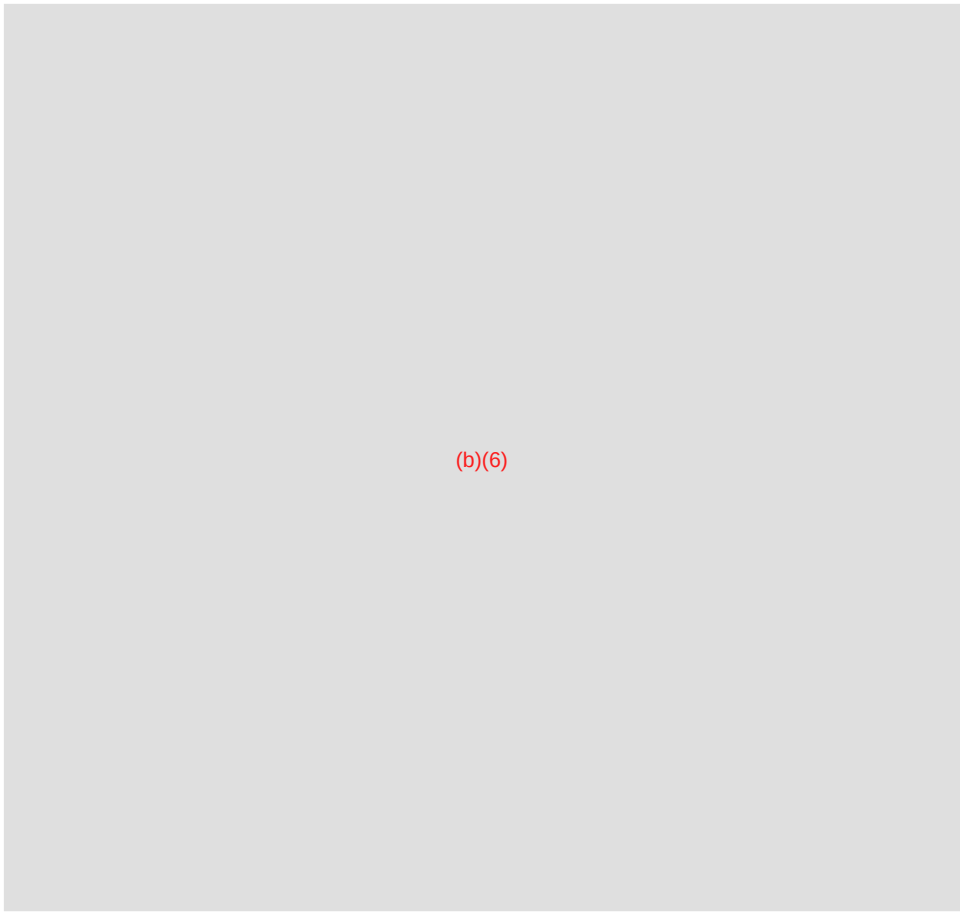




17JUL15

SUBJ: CAFO KEY PERSONNEL LISTING **CORRECTED COPY**





DISTRIBUTION
INFO: CAFO/WWSSD

FOR OFFICIAL USE ONLY
PAGE 3 LAST (b)(6)

2126692 14:54 20151104 IN:SSDEMAIL #4 OUT:NCISWWSSD #3

GENERAL ADMINISTRATION 04NOV15

FROM: 0000 GEN: 00-0017

TO: DIST

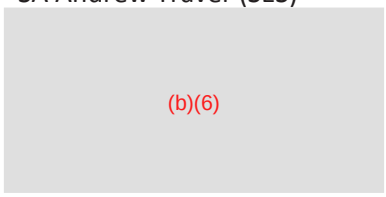
SUBJ: NCIS 2 (CODE 00) EXECUTIVE STAFF KEY PERSONNEL

MAILING ADDRESS

Naval Criminal Investigative Service
Russell-Knox Building
27130 Telegraph Road
Quantico, VA 22134
(571) 305-9000 (Front Office)
(571) 305-9115 (Facsimile)

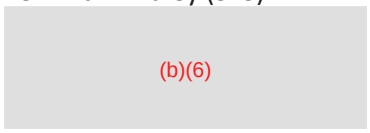
SENIOR LEADERSHIP

Director
SA Andrew Traver (SES)



Executive Assistant, Director

Deputy Director
SA Mark Ridley (SES)



(b)(6)

Executive Assistant, Deputy Director

(b)(6)

Principal Executive Assistant Director, Management & Administration SA Samuel Worth (SES)

(b)(6)

FOR OFFICIAL USE ONLY
PAGE 1

04NOV15

SUBJ: NCIS 2 (CODE 00) EXECUTIVE STAFF KEY PERSONNEL

(b)(6)

Executive Assistant, Principal Executive Assistant Director, Management & Administration SA (b)(6)

(b)(6)

Executive Assistant Director, Global Operations Directorate SA Rod Baldwin (SES)

(b)(6)

Executive Assistant, Executive Assistant Director, Global Operations Directorate SA (b)(6)

(b)(6)

Senior Intelligence Officer 02G/ Global Operations Mr. (b)(6)

(b)(6)

Executive Assistant Director, Criminal Investigations and Operations Directorate SA Andy Hogan (SES)

(b)(6)

Assistant Director, Criminal Investigations and Operations Directorate SA (b)(6)

(b)(6)

Executive Assistant Director, Intelligence and Information Sharing Directorate SA Chris Cote (DISL)

04NOV15

SUBJ: NCIS 2 (CODE 00) EXECUTIVE STAFF KEY PERSONNEL

(b)(6)

Senior Intelligence Officer, Intelligence and Information Sharing Directorate Mr. Rick Karakadze (DISL)

(b)(6)

Assistant Director, Intelligence and Information Sharing Directorate SA Mark Russ

(b)(6)

(b)(6)

Executive Assistant Director, Atlantic Operations SA Chuck May (SES)

(b)(6)

Executive Assistant, Executive Assistant Director, Atlantic Operations SA (b)(6)

(b)(6)

Acting Executive Assistant Director, Pacific Operations SA (b)(6)

(b)(6)

Executive Assistant, Executive Assistant Director, Pacific Operations Vacant

(b)(6)

Acting Executive Assistant Director, National Security Directorate SA (b)(6)

(b)(6)

04NOV15

SUBJ: NCIS 2 (CODE 00) EXECUTIVE STAFF KEY PERSONNEL

Chief, Strategic Planning

(b)(6)

(b)(6)

Principal Computer Scientist, Strategic Planning Mr. Edward So (DISL)

(b)(6)

Senior Advisor, Congressional and Media Affairs Mr. (b)(6)

(b)(6)

Senior Policy Advisor

(b)(6)

EXECUTIVE STAFF

Chief of Staff

(b)(6)

Executive Writer and Editor

(b)(6)

Inspector General

(b)(6)

Counsel

04NOV15

SUBJ: NCIS 2 (CODE 00) EXECUTIVE STAFF KEY PERSONNEL

(b)(6)

Comptroller

(b)(6)

Communications Director

(b)(6)

Ombudsman

(b)(6)

Senior Representative, SECNAV/OPNAV Staffs SA (b)(6)

(b)(6)

Assistant Director, Human Resources Directorate SA (b)(6)

(b)(6)

Security Manager

(b)(6)

Assistant Director, Command Information Officer, Information Systems Directorate Mr. (b)(6)

(b)(6)

04NOV15

SUBJ: NCIS 2 (CODE 00) EXECUTIVE STAFF KEY PERSONNEL

(b)(6)

Assistant Director - Manpower, Planning and Support Mr (b)(6)

(b)(6)

Commanding Officer, Office of Military Support CAPT (b)(6)

(b)(6)

Senior Representative, USMC HQ Staff

(b)(6)

Supervisory Executive Assistant

(b)(6)

Lead Executive Staff Assistant

(b)(6)

Executive Staff Assistant
Vacant

(b)(6)

Executive Staff Assistant (Pentagon)

(b)(6)

Distribution:
NCISHQ: ALL DEPARTMENTS AND DIRECTORATES
INFO: WWSSD/AFLT

FOR OFFICIAL USE ONLY
PAGE 6 LAST (b)(6)

2181088 09:39 20151201 IN:SSDEMAIL #5 OUT:NCISWWSSD #4

GENERAL ADMINISTRATION 01DEC15

FROM: 011C GEN: 11C-0027

TO: DISTRIBUTION

SUBJ: MANPOWER, PLANNING AND SUPPORT DIRECTORATE KEY PERSONNEL AND DATA SHEET

NCIS-2: MANPOWER, PLANNING AND SUPPORT DIRECTORATE KEY PERSONNEL AND DATA SHEET

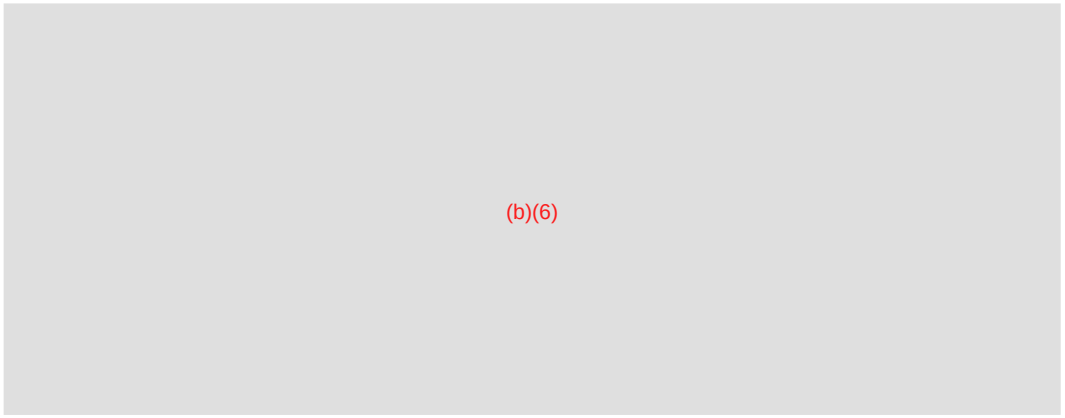
MAILING ADDRESS
NAVAL CRIMINAL INVESTIGATIVE SERVICE HQ
ATTN: CODE 11C
27130 TELEGRAPH ROAD
QUANTICO, VA 22134

Manpower, Planning & Support (MPS)

(b)(6)

11A - SECURITY & FACILITIES

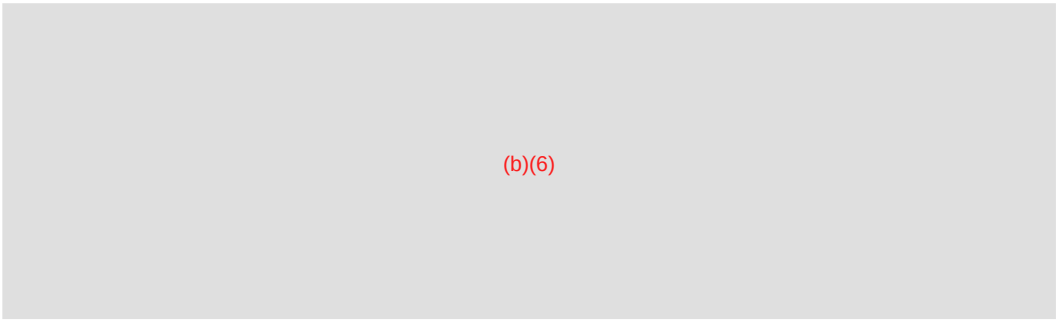
(b)(6)



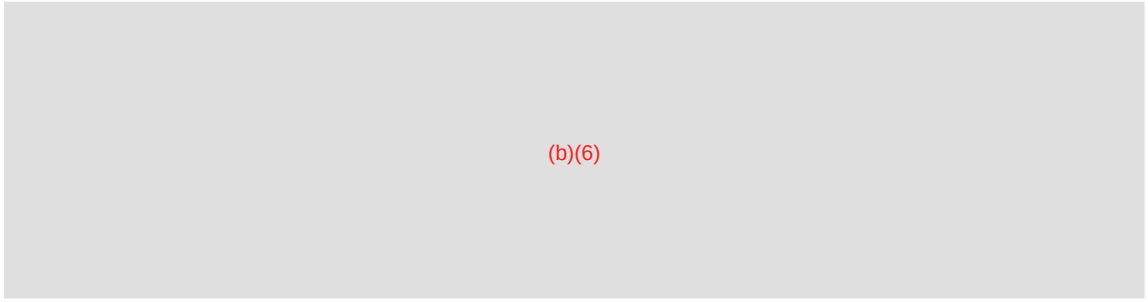
01DEC15

SUBJ: MANPOWER, PLANNING AND SUPPORT DIRECTORATE KEY PERSONNEL AND D

11A3



11B - ACQUISITION & LOGISITICS



(b)(6)

Procurement Analyst

11B1

(b)(6)

11B2
VACANT
Chief, Logistics Division

(b)(6)

(b)(6)

(b)(6)

Arms & Ammunition Branch Mgr.

(b)(6)

Supply & Services Branch Mgr.

11C - ADMINISTRATIVE SERVICES & RECORDS MANAGEMENT

(b)(6)

Office Manager

(b)(6)

01DEC15

SUBJ: MANPOWER, PLANNING AND SUPPORT DIRECTORATE KEY PERSONNEL AND D

(b)(6)

11C1 - RECORDS MANAGEMENT

(b)(6)

Branch Head, Records Management

(b)(6)

Supervisor, Liaison Section

VACANT

(b)(6)

Supervisor, Imaging Section

11C2 - CENTRAL ADMINISTRATION

(b)(6)

14A - PLANNING & EVALUATION

(b)(6)

Evaluation Lead

14P - FISCAL PLANNING & MANPOWER

(b)(6)

2185547 12:33 20151202 IN:SSDEMAIL #7 OUT:NCISWWSSD #2

GENERAL ADMINISTRATION 02DEC15

FROM: 0000 GEN: 15-0003

TO: DIST

SUBJ: NCIS-2 (CODE 15) INFORMATION TECHNOLOGY (IT) DIRECTORATE
KEY PERSONNEL DATA SHEET

MAILING ADDRESS
NAVAL CRIMINAL INVESTIGATIVE SERVICE
ATTN: CODE 15
RUSSELL-KNOX BUILDING
27130 TELEGRAPH ROAD
QUANTICO, VA 22134

UNCLAS FAX: 571-305-9994

IT SOLUTIONS CENTER: 571-305-9999
ITSC@ncis.navy.mil

Navy-ITWatch Desk
(Afterhours ITSC - Help Desk)
COML: 571-305-9438
DSN: 310-240-9438
UNCLAS FAX: COML: 571-305-9431

(b)(6)

POSITION/CODE	KEY PERSONNEL
Assistant Director/ Chief Information Officer	(b)(6)
Deputy Assistant Director Information Management	

Supervisory Program Anal
Administrative Managem

Division Chief
IT Governance (15A1)

Division Chief
Enterprise Security (15A2)

Deputy Assistant Director
Chief Technology Officer (

Division Chief
IT Project Management (1

Division Chief
Technology development

(b)(6)

Deputy Assistant Director
Enterprise Services (15C)

Division Chief
IT Operations (15C1)

Supervisory IT Specialist
IT System ADMN Branch (

Supervisory Telecommuni
IT Network/Messaging Su

Division Chief
IT Services (15C2)

Supervisory IT Specialist
Regional Computer Spec

Supervisory IT Specialist
Regional Computer Spec

Deputy Assistant Directo
IT Consolidated Support

(b)(6)

Division Chief
Information Assurance (

Division Chief
Network Operations (ITC

DISTRIBUTION
INFO: WWSSD

FOR OFFICIAL USE ONLY
PAGE 1 LAST (b)(6)

2103997 00:56 20151027 IN:SSDEMAIL #2 OUT:NCISWWSSD #1

GENERAL ADMINISTRATION 27OCT15

FROM: FEAJ GEN: AJ-0002

TO: DISTRIBUTION

SUBJ: NCIS-2 CHANGE OF ADCON/OPCON FOR USS RONALD REAGAN (CVN-76)

NOTE: NCISRA USS RONALD REAGAN HAS TRANSFERRED TO THE FAR EAST AREA OF RESPONSIBILITY. FEFO HAS ASSUMED ADCON/OPCON FOR USS RONALD REAGAN (CVN-76)

ADCON: FEFO OPCON: FEFO

PARENT NCISFO: FEFO
PARENT NCISRA: FEAJ

USS RONALD REAGAN (CVN-76) is no longer homeported in San Diego, California, and as of 01Oct15, is homeported in Yokosuka, Japan. The previous Consolidated Law Enforcement Operations Center (CLEOC) code SWXP, assigned to NCISRU RONALD REAGAN (CVN-76), is no longer accurate or valid. Due to the imminent implementation of the Navy Justice Information System (NJIS), no new CLEOC code for NCISRU RONALD REAGAN (CVN-76) will be created by NCISHQ. Therefore, for administrative purposes and oversight during the interim period, all leads intended for NCISRU RONALD REAGAN (CVN-76) should be directed to FEAJ for completion.

MAILING ADDRESS:
NCISRU RONALD REAGAN (CVN-76)
ATTN SPECIAL AGENT AFLOAT
USS RONALD REAGAN (CVN-76)
FPO AP 96616

(b)(6)

EMAIL (NCIS)
(b)(6) @ncis.navy.mil

UIC: 21412

DISTRIBUTION
WWSSD

FOR OFFICIAL USE ONLY
PAGE 1 LAST (b)(6)

1699527 08:57 20150602 IN:SSDEMAIL #1 OUT:NCISWWSSD #1

GENERAL ADMINISTRATION 02JUN15

FROM: CBFO GEN: CYB-0001

TO: DIST

SUBJ: CYBER OPERATIONS FIELD OFFICE KEY PERSONNEL (CBFO)

CYBER OPERATIONS FIELD OFFICE-(CBFO)

TITLE	PERSONNEL	CONTACT NUMBERS
SAC		
FOS		
SIS		

(b)(6)

ATLANTIC CYBER OPERATIONS-(CBAW)

TITLE	PERSONNEL	CONTACT NUMBERS
ASA Atla		
SSA Wa		
SSA Wa		

(b)(6)

SSA
Nor (b)(6)

FOR OFFICIAL USE ONLY
PAGE 1

02JUN15

SUBJ: DFLSDJFS

PACIFIC CYBER OPERATIONS - (CBPW)
TITLE PERSONNEL CONTACT NUMBERS

ASA
Paci

SSA (b)(6)

FOR OFFICIAL USE ONLY
PAGE 1

29APR14

SUBJ: CYBER OPERATIONS FIELD OFFICE KEY PERSONNEL (CBFO)

SSA (b)(6)

SSA (b)(6)

DISTRIBUTION
NCISHQ: ALL Departments and Directorates
INFO: WWSSD/AFLT

FOR OFFICIAL USE ONLY
PAGE 2 LAST (b)(6)

1906532 18:37 20150812 IN:SSDEMAIL #5 OUT:NCISWWSSD #1

GENERAL ADMINISTRATION 12AUG15

FROM: 002P GEN: O2P-0001

TO: DIST

SUBJ: EXECUTIVE ASSISTANT DIRECTOR FOR PACIFIC OPERATIONS KEY PERSONNEL LISTING

MAILING ADDRESS:

(b)(6)

DMS PLA: NAVCRIMINVSERV EADPAC SAN DIEGO CA

TELEPHONES: COMMERCIAL: (CONUS 011) DSN: (312) UNCLAS PHONE: 619 553 6835
UNCLAS FAX: 619 553-7048

EADPAC
OFFICE:
COMM
CELL: (b)(6)

CHIEF STAFF OFFICER (b)(6)
OFFICE:
COMME (b)(6)
CELL:

EXECUTIVE ASSISTANT (b)(6)
OFFICE:
COMME (b)(6)
CELL:

EXECUTIVE SECRETARY (b)(6)
OFFICE:
COMMER (b)(6)
CELL: TBD

PSYCHOLOGIST DR. (b)(6)
OFFICE:
COMME (b)(6)
CELL:

DESK OFFICER (VACANT)
OFFICE:
COMMER (b)(6)
CELL: TBD

DESK OFFICER (VACANT) - (incoming (b)(6)
OFFICE: (b)(6)

FOR OFFICIAL USE ONLY
PAGE 1

12AUG15

SUBJ: EXECUTIVE ASSISTANT DIRECTOR FOR PACIFIC OPERATIONS KEY PERSON

COMMERCIAL: (b)(6)
CELL: TBD

DESK OFFICER SA (b)(6)
OFFICE:
COMME (b)(6)
CELL:

STAFF JUDGE ADVOCATE LT (b)(6)
OFFICE:
COMME (b)(6)
CELL:

SENIOR INTEL OFFICER (b)(6)
OFFICE:
COMMER (b)(6)
CELL: TBD

C-CICA
OFFICE (b)(6)

COMME (b)(6)
CELL:

FOR OFFICIAL USE ONLY
PAGE 2 LAST (b)(6)

GENERAL ADMINISTRATION 18FEB16

FROM: FESS GEN: SS-0001

TO: DIST

SUBJ: NCIS-2 (FEX6) NCISRU USS BONHOMME RICHARD (LHD-6) DATA SHEET

ADCON: FEFO
OPCON: FEFO

PARENT NCISFO: FEFO
PARENT NCISRA: FESS

NOTE: LEADS SHOULD BE DIRECTED TO FEX6 WITH AN INFORMATION COPY TO NCISRA SASEBO, JAPAN (FESS). PRIOR TO SENDING LEADS TO FEX6, CONTACT FESS VIA DSN PHONE AT 315-252-3621.

MAILING ADDRESS:

(b)(6)

TELEPHONE DSN
OFFICE 315-453-7245

UIC: 34451

DISTRIBUTION
INFO: WWSSD

FOR OFFICIAL USE ONLY
PAGE 1 LAST (b)(6)

1501974 16:32 20150316 IN:SSDEMAIL #3 OUT:NCISWWSSD #1

GENERAL ADMINISTRATION 16MAR15

FROM: HIFO GEN: HN-0003

TO: DIST

SUBJ: NCIS-2/(HIFO) NCISFO HAWAII KEY PERSONNEL LISTING

CODE/POSITION KEY PERSONNEL

SAC

ASAC
(CRIM)

(NSD)

(b)(6)

SIO

FOSO

SSA (CRIM

SSA (HIKH)

(b)(6)

FOR OFFICIAL USE ONLY
PAGE 1

16MAR15

SUBJ: NCIS-2/(HIFO) NCISFO HAWAII KEY PERSONNEL LISTING

SSA (HIMI)

SPA

EVID
CUSTODIA

FCS

(b)(6)

PACOM

(b)(6)

PACFLT

CI SUPPORT ELEMENT TO PACOM
SA

JTTF
SA

(b)(6)

2GJV

16MAR15

SUBJ: NCIS-2/(HIFO) NCISFO HAWAII KEY PERSONNEL LISTING

(b)(6)

2GTH
SA

(b)(6)

FORENSIC CONSULTANT (b)(6)
SA

(b)(6)

INFO: WWSSD

1753292 07:47 20150618 IN:SSDEMAIL #2 OUT:NCISWWSSD #1

GENERAL ADMINISTRATION 18JUN15

FROM: MEBJ GEN: BJ-0015

TO: DIST

SUBJ: NICS-2: (MEFO) NCIS MIDDLE EAST FIELD OFFICE KEY PERSONNEL

CODE: MEBJ
COMM FROM THE U.S.: 011 + COUNTRY CODE + TEL # MOBILE FROM THE U.S.: 011 + COUNTRY CODE + CELL# WITHIN THE MIDDLE EAST OR FROM EUROPE: 00 + COUNTRY CODE + TEL # DSN PREFIX FOR BAHRAIN: 318

POSITION KEY PERSONNEL

(b)(6)

(b)(6)

SSA FP/TMU VACANT (b6 INBOUND 7/15)

(b)(6)

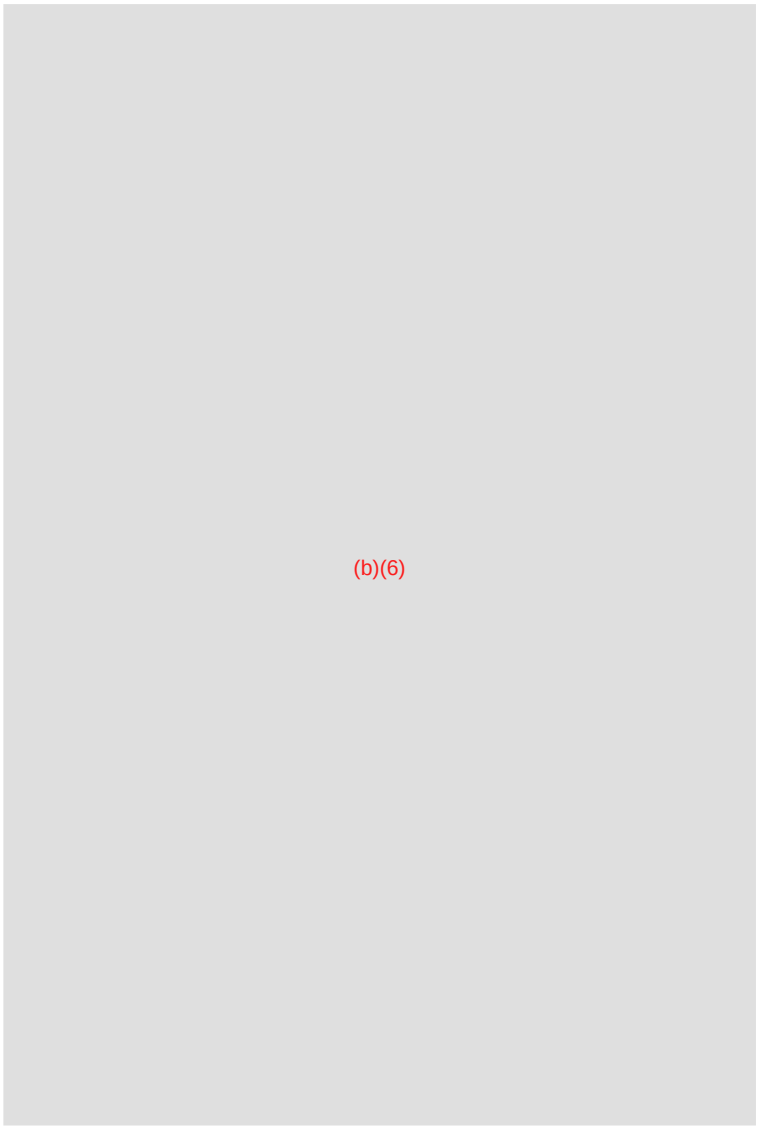
FOR OFFICIAL USE ONLY
PAGE 1

18JUN15

SUBJ: NICS-2: (MEFO) NCIS MIDDLE EAST FIELD OFFICE KEY PERSONNEL

(b)(6)

(b)(6)



18JUN15

SUBJ: NICS-2: (MEFO) NCIS MIDDLE EAST FIELD OFFICE KEY PERSONNEL

(b)(6)

(b)(6)

DISTRIBUTION
NCISHQ: ALL DIRECTORATES AND DEPARTMENTS
INFO: WWSSD/MEBJ

2363892 02:07 20160207 IN:SSDEMAIL #1 OUT:NCISWWSSD #1

GENERAL ADMINISTRATION 07FEB16

FROM: MEBJ GEN: BJ-0003

TO: DIST

SUBJ: NCIS-2: (MEKP) NCIS MIDDLE EAST FIELD OFFICE KEY PERSONNEL

CODE: MEBJ

DIALING INSTRUCTIONS:
FROM THE US: 011 + COUNTRY CODE + TEL#
WITHIN THE MIDDLE EAST/EUROPE: 00 + COUNTRY CODE + NUMBER DSN PREFIX FOR BAHRAIN: 318

MIDDLE EAST FIELD OFFICE KEY PERSONNEL

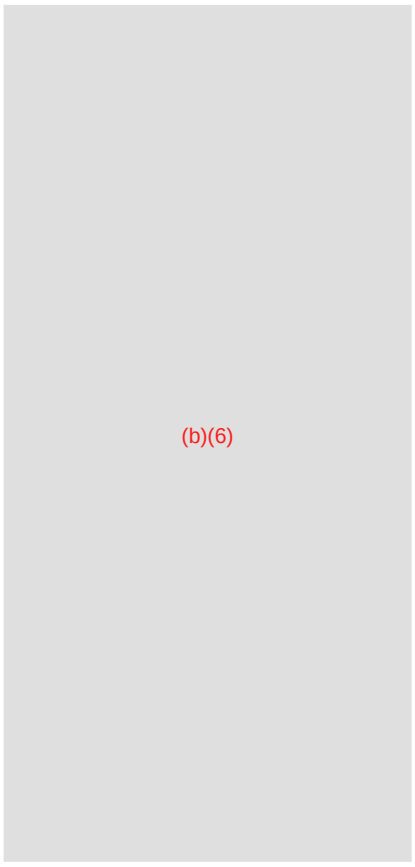
(b)(6)

CHIEF TRANSNATIONAL CRIMES UNIT (TCU) (b)(6)

(b)(6)

07FEB16

SUBJ: NCIS-2: (MEKP) NCIS MIDDLE EAST FIELD OFFICE KEY PERSONNEL



MEDB - NCISRA DUBAI, UAE

(b)(6)

MEDJ - NCISRA DJIBOUTI

(b)(6)

MEDJ

(b)(6)

MEEG - FPD EGYPT

(b)(6)

MEUM - FPD MAURITIUS

(b)(6)

07FEB16

SUBJ: NCIS-2: (MEKP) NCIS MIDDLE EAST FIELD OFFICE KEY PERSONNEL

MEKE - FPD KENYA

(b)(6)

FPD JORDAN

(b)(6)

DISTRIBUTION
INFO: WWSSD

FOR OFFICIAL USE ONLY

2262017 15:47 20160105 IN:SSDEMAIL #20 OUT:NCISWWSSD #15

GENERAL ADMINISTRATION 05JAN16

FROM: NENP GEN: NP-0002

TO: DIST

SUBJ: NCIS-2/(NEBN BOSTON-JTTF) NCIS REPRESENTATIVE TO THE FBI
JOINT TERRORIST TASK FORCE (JTTF) DATA SHEET

NOTE: ANY NCIS CAT 5 INVESTIGATIVE LEADS TO THE NEBN BOSTON-JTTF REP SHOULD ALSO INCLUDE THE FCI SSA AT NENP AND THE FCI ASAC AT NENP ON DISTRIBUTION FOR CASE TRACKING AND ADMINISTRATIVE PURPOSES.

PARENT NCISFO: NORTHEAST FIELD OFFICE, NEWPORT, RI PARENT NCISRA: NEWPORT, RI (NENP)

MAILING & LOCAL ADDRESS
NCIS REPRESENTATIVE

(b)(6)

TELEPHONES	COMMERICAL
DIRECT LINE (NCIS REP)	(617) 223-6452
GENERAL NUMBER	(617) 742-5533
AGENTS CELL	b6

UNCLAS FACSIMILE (NCIS REP) (617) 223-6545

NMSG PLA: NONE
USE: NAVCRIMINVSERVFO NORTHEAST NEWPORT RI NCIC/NLETS ORI: NONE
UIC: 67985

AFTER HOURS (617) 742-5533
(FBI BOS DUTY AGENT AND OPERATIONS CENTER)

THE FBI/BOSTON OPERATIONS CENTER DUTY AGENT CAN REACH THE NCIS REPRESENTATIVE TO THE JTTF, SQUAD CT-1.

COVERAGE:
THE FBI JTTF HAS JURISDICTIONAL RESPONSIBILITY FOR CONDUCTING BOTH DOMESTIC AND INTERNATIONAL COUNTERTERRORISM INVESTIGATIONS WITHIN THE CONFINES OF THE CITY OF BOSTON AND SURROUNDING COUNTIES (SUFFOLK COUNTY, SOUTHERN ESSEX AND MIDDLESEX COUNTIES, NORTHERN NORFOLK AND PLYMOUTH COUNTIES)

DISTRIBUTION
INFO: WWSSD

FOR OFFICIAL USE ONLY
PAGE 1 LAST (b)(6)

2261210 13:11 20160105 IN:SSDEMAIL #9 OUT:NCISWWSSD #8

GENERAL ADMINISTRATION 28DEC15

FROM: NENP GEN: NP-0010

TO: DIST

SUBJ: NCIS-2: (NECA/CNCL) NCISRU CRANE DATA SHEET

PARENT NCISFO: NORTHEAST FIELD OFFICE, NEWPORT, RI (NENP) PARENT NCISRA: GREAT LAKES, IL (NEGL)

NOTE: NCISRU CRANE IN is no longer under the ADCON/OPCON of Central Field Office as of 01NOV15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNCA, assigned to NCISRA CRANE IL, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code NECA/NCISRU CRANE IN will not be used until NJIS comes online. Please copy NENP, as appropriate. All other correspondence will utilize NECA

MAILING ADDRESS/LOCAL ADDRESS
NCISRU CRANE
NSWC 300 HWY 361
BLDG 121 RM 214
CRANE IN 47522-5000

TELEPHONES COMMERCIAL DSN
OFFICE: (812)854-4402 482-4402
UNCLAS FAX: (812)854-3461 482-3461
STU-III: b7E
AFTER HOURS: (812)854-3300 482-3300

NMSG PLA: NAVCRIMINVSERVREP CRANE IN
NLET/NCIC ORI: NONE
UIC: NONE - USE NEGL: 42919

TERRITORIAL COVERAGE:
FCI COVERAGE AS DIRECTED BY NCISFO NORTHEAST

PRINCIPAL INSTALLATIONS SERVICED:
NSWC CRANE DIVISION, CRANE, IN
NSWC DET LOUISVILLE, KY

DISTRIBUTION
WWSSD

2261217 13:13 20160105 IN:SSDEMAIL #11 OUT:NCISWWSSD #10

GENERAL ADMINISTRATION 28DEC15

FROM: NENP GEN: NP-0009

TO: DIST

SUBJ: NCIS-2: (NECL/CNCL) NCISRU CLEVELAND DATA SHEET

PARENT NCISFO: NORTHEAST FIELD OFFICE, NEWPORT, RI (NENP) PARENT NCISRA: GREAT LAKES, IL (NEGL)

NOTE: NCISRU CLEVELAND OH is no longer under the ADCON/OPCON of Central Field Office as of 01OCT15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNCL, assigned to NCISRA CLEVELAND OH, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code NECL/NCISRU CLEVELAND OH will not be used until NJIS comes online. Please copy NEFO, as appropriate. All other correspondence will utilize NECL

MAILING ADDRESS LOCAL ADDRESS
P. O. BOX 99809 1240 E. 9TH ST, RM 1457
CLEVELAND, OH 44199-2055 CLEVELAND, OHIO 44199-2055

TELEPHONES COMMERCIAL DSN
OFFICE: (216) 522-6774/5/6758 580-6774/5/6758 UNCLAS FACSIMILE: (216) 522-6629
STU-III: b7E
AFTERHOURS: (216) 522-5666/23
DFAS CLEVELAND COMMUNICATIONS CENTER

NMSG PLA: none
use - NAVCRIMINVSERVFO NORTHEAST NEWPORT RI NCIC/NLETS ORI: none
UIC: NONE; USE NEGL - 42919

TERRITORIAL COVERAGE
OHIO: NON HAZARDOUS INTERVIEWS ONLY
NOTE: NCISRU CLEVELAND OH CONSISTS OF ONE (1) GS-1810 INVESTIGATOR.

PRINCIPAL INSTALLATION SERVICED
DFAS CLEVELAND OH
DFAS COLUMBUS OH

BUPERS PCS COMPONENT

DISTRIBUTION
WWSSD

FOR OFFICIAL USE ONLY
PAGE 1 LAST (b)(6)

2261711 14:23 20160105 IN:SSDEMAIL #18 OUT:NCISWWSSD #14

GENERAL ADMINISTRATION 28DEC15

FROM: NENP GEN: NP-0012

TO: DIST

SUBJ: NCIS-2: "CORRECTED COPY" (NEDY/CNDY) NCISRU DAYTON DATA SHEET

********** CI COVERAGE ONLY **********

PARENT NCISFO: NORTHEAST FIELD OFFICE, NEWPORT, RI (NENP) PARENT NCISRA: GREAT LAKES, IL (NEGL)

NOTE: NCISRU DAYTON OH is no longer under the ADCON/OPCON control of Central Field Office as of 01OCT15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNDY, assigned to NCISRU DAYTON OH, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code NEDY/NCISRU DAYTON OH will not be used until NJIS comes online. Please copy NEFO, as appropriate. All other correspondence will utilize NEDY.

MAILING ADDRESS LOCAL ADDRESS
NCIS REPRESENTATIVE NCISRU DAYTON
AFOSI REGION 1/XOQ 4375 CHIDLAW RD, BLDG 216, RM A036
4375 CHIDLAW ROAD, DOOR S007 WRIGHT PATTERSON AFB, OH 45433-5006
WRIGHT PATTERSON AFB, OH 45433-5006

TELEPHONES COMMERCIAL DSN

OFFICE STE: 937-522-2187 672-2187
CELL PHONE: 202-372-7837
FACSIMILE: 937-522-2197 (PLEASE USE FAX COVER SHEET)
SECURE FAX: (b)(6)
SSD TELECOMMUNICATIONS: NIPRNET
NMSG PLA: NAVCRIMINVSERVRA DAYTON OH
NCIS/NLET ORI NONE
UIC: 34402

TERRITORIAL COVERAGE:
EASTERN KENTUCKY AND OHIO

PRINCIPAL INSTALLATION SERVICED:
WRIGHT PATTERSON AFB, OH

DISTRIBUTION
WWSSD

FOR OFFICIAL USE ONLY
PAGE 1 LAST (b)(6)

2261154 13:07 20160105 IN:SSDEMAIL #8 OUT:NCISWWSSD #7

GENERAL ADMINISTRATION 28DEC15

FROM: NENP GEN: NP-0013

TO: DIST

SUBJ: NCIS-2: (NEGL/CNGL) NCISRA GREAT LAKES DATA SHEET

PARENT NCISFO: NORTHEAST FIELD OFFICE, NEWPORT, RI (NENP)

NOTE: NCISRA GREAT LAKES IL is no longer under the ADCON/OPCON control of Central Field Office as of 01NOV15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNGL, assigned to NCISRA GREAT LAKES IL, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code NEGL/NCISRA GREAT LAKES IL will not be used until NJIS comes online. Please copy NENP, as appropriate. All other correspondence will utilize NEGL.

MAILING ADDRESS	LOCAL ADDRESS
2540A PAUL JONES ST	2540A PAUL JONES ST
GREAT LAKES, IL 60088	GREAT LAKES, IL 60088

TELEPHONES	COMMERCIAL	DSN
OFFICE:	(847) 688-5655/6/7/5668/9	792-655/6/7/5668/9
AFTER HOURS:	(847) 688-5555	
GREAT LAKES PD: 792-5555		
PATCH NUMBER:	(847) 688-0147 CONNECT: *DISCONNECT: #	
UNCLAS FACSIMILE:	(847) 688-2636	792-2636
STE:	b7E	b7E

NMSG PLA: NAVCRIMINVSERVRA GREAT LAKES IL//CNGL// NCIC/NLETS ORI: NONE BASE STATION IDENTIFIER CODE (NFC): 320
UIC: 42919

TERRITORIAL COVERAGE:
INDIANA, ILLINOIS, MICHIGAN, WISCONSIN, OHIO, KENTUCKY

PRINCIPAL INSTALLATIONS SERVICED:
AIR FORCE OFFICE OF SPECIAL INVESTIGATIONS TENTH FIELD INVESTIGATIONS SQUADRON, INDIANAPOLIS, IN BUREAU OF NAVAL PERSONNEL PERMANENT CHANGE OF STATION COMPONENT,

CLEVELAND, OH DEFENSE CONTRACT MANAGEMENT AGENCY (DCMA) OFFICES IN WISCONSIN, ILLINOIS, INDIANA AND MICHIGAN DEFENSE FINANCE AND ACCOUNTING SERVICE, CLEVELAND, OH DEFENSE FINANCE AND ACCOUNTING SERVICE, COLUMBUS, OH DEFENSE FINANCE AND ACCOUNTING SERVICE INDIANAPOLIS, IN DEFENSE INFORMATION SYSTEMS AGENCY, SCOTT AFB IL DEFENSE REUTILIZATION & MARKETING REGION BATTLECREEK, MI DOD-IG DEFENSE CRIMINAL INVESTIGATIVE SERVICE (DCIS) RESIDENT AGENCY,

28DEC15

SUBJ: NCIS-2: (NEGL/CNGL) NCISRA GREAT LAKES DATA SHEET

INDIANAPOLIS, IN
MARINE OFFICER SELECTION OFFICE COLUMBUS, OH MILITARY ENTRANCE PROCESSING COMMAND, GREAT LAKES, IL NAVY AND MARINE CORPS RESERVE CENTER COLUMBUS, OH NAVAL DENTAL CLINIC GREAT LAKES, IL NAVAL STATION, GREAT LAKES, IL NAVAL SURFACE WARFARE CENTER CRANE DIVISION, CRANE, IN NAVAL SURFACE WARFARE CENTER DET LOUISVILLE, KY NAVY DENTAL RESEARCH INSTITUTE GREAT LAKES, IL NAVY EXCHANGE, GREAT LAKES, IL NAVY LEGAL SERVICE OFFICE, GREAT LAKES, IL NAVY OPERATIONAL SUPPORT CENTER, DECATUR, IL NAVY OPERATIONAL SUPPORT CENTER, PEORIA, IL NAVY OPERATIONAL SUPPORT CENTER, ROCK ISLAND, IL NAVY OPERATIONAL SUPPORT CENTER, INDIANAPOLIS, IN NAVY OPERATIONAL SUPPORT CENTER, LOUISVILLE, KY NAVY OPERATIONAL SUPPORT CENTER, BATTLE CREEK, MI NAVY OPERATIONAL SUPPORT CENTER, DETROIT, MI NAVY OPERATIONAL SUPPORT CENTER, SAGINAW, MI NAVY OPERATIONAL SUPPORT CENTER, AKRON, OH NAVY OPERATIONAL SUPPORT CENTER, CINCINNATI, OH NAVY OPERATIONAL SUPPORT CENTER, COLUMBUS, OH NAVY OPERATIONAL SUPPORT CENTER, TOLEDO, OH NAVY OPERATIONAL SUPPORT CENTER, YOUNGSTOWN, OH NAVY OPERATIONAL SUPPORT CENTER, GREEN BAY, WI NAVY OPERATIONAL SUPPORT CENTER, MADISON, WI NAVY OPERATIONAL SUPPORT CENTER, MILWAUKEE, WI NAVY REGION MID-ATLANTIC RESERVE COMPONENT COMMAND, GREAT LAKES, IL NAVY RECRUIT TRAINING COMMAND, GREAT LAKES, IL NAVY RECRUITING DISTRICT COLUMBUS, OH NAVY RECRUITING DISTRICT DETROIT, MI NAVY RECRUITING AREA FIVE, GREAT LAKES, IL NAVY RECRUITING DISTICT INDIANAPOLIS IN NAVY RECRUITING DISTRICT, MILWAUKEE, WI NAVY TRAINING CENTER, GREAT LAKES, IL PERSONNEL SUPPORT DETACHMENT, COLUMBUS, OH PERSONNEL SUPPORT DETACHMENT, GREAT LAKES, IL SERVICE SCHOOL COMMAND, GREAT LAKES, IL TRANSIENT PERSONNEL UNIT, GREAT LAKES, IL WRIGHT PATTERSON AIR FORCE BASE, OH

DISTRIBUTION
WWSSD

2261596 14:06 20160105 IN:SSDEMAIL #14 OUT:NCISWWSSD #13

GENERAL ADMINISTRATION 28DEC15

FROM: NENP GEN: NP-0011

TO: DIST

SUBJ: NCIS-2: "CORRECTED COPY" (NEIN/CNIN) NCISRU INDIANAPOLIS
DATA SHEET

PARENT NCISFO: NORTHEAST FIELD OFFICE, NEWPORT, RI (NENP) PARENT NCISRA: GREAT LAKES, IL (NEGL)

NOTE: NCISRU INDIANAPOLIS IN is no longer under the ADCON/OPCON of Central Field Office as of 01NOV15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNIN, assigned to NCISRU INDIANAPOLIS IN, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code NEIN/NCISRU INDIANAPOLIS IN will not be used until NJIS comes online. Please copy NENP, as appropriate. All other correspondence will utilize NEIN.

MAILING/LOCAL ADDRESS
NCISRU INDIANAPOLIS (FRAUD)
AFOSI 10TH FIS OPERATING L-A
111 MONUMENT CIRCLE SUITE 412
INDIANAPOLIS, IN 46204

TELEPHONES COMMERCIAL
OFFICE: (317) 226-5380
AFTER HOURS: (847) 456-4576
UNCLAS FACSIMILE: (317) 226-5134

NMSG PLA: NONE
USE - NAVCRIMINVSERVFO NORTHEAST NEWPORT RI
UIC: 34409

TERRITORIAL COVERAGE:
ONLY MAJOR PROCUREMENT FRAUD INVESTIGATIONS/LEAD COVERAGE IN THE STATES OF INDIANA, OHIO, AND MICHIGAN.

PRINCIPAL INSTALLATIONS SERVICED:

AIR FORCE OSI TENTH FIELD INVESTIGATIONS SQUADRON, INDIANAPOLIS DETACHMENT; DEFENSE FINANCE AND ACCOUNTING SERVICE INDIANAPOLIS, IN; DOD-IG DEFENSE CRIMINAL INVESTIGATIVE SERVICE (DCIS) RESIDENT AGENCY, INDIANAPOLIS, IN; DEFENSE CONTRACT MANAGEMENT AGENCY (DCMA) OFFICES IN WISCONSIN, ILLINOIS, INDIANA AND MICHIGAN.

DISTRIBUTION
WWSSD

FOR OFFICIAL USE ONLY
PAGE 1 LAST (b)(6)

GENERAL ADMINISTRATION 03FEB16

FROM: NFNF GEN: NF-0002

TO: DIST

SUBJ: NCIS - 2 (NFNF) NCISRA NORFOLK VA DATA SHEET

PARENT NCISFO: NFFO

NOTE SUBORDINATE OFFICES: NFCE, NFFM, NFHV, NFLC, NFPV, NFYT, NFXA, NFXH, NFXL, NFXO, NFXQ, NFX1, NFX3

NOTE: NCIS OFFICES UNDER NCISRA NORFOLK ARE SERVICED BY THE NCIS CENTRAL EVIDENCE FACILITY (CEF) AND EVIDENCE SHOULD BE MAILED DIRECTLY TO THEM AT: 9079 HAMPTON BLVD, SUITE 110, NORFOLK VA 23505-1098. THE LONG TERM STORAGE (LTS) FACILITY IS STILL PENDING THE TESTING AND IMPLEMENTATION OF AN ELECTRONIC CUSTODY SYSTEM. FURTHER GUIDANCE IS PENDING.

MAILING ADDRESS LOCAL ADDRESS

NCIS NORFOLK FIELD OFFICE
1329 BELLINGER BLVD
NORFOLK VA 23511-2310

(b)(6)

TELEPHONES:

OFFICE: (757) 444-7327 DSN: 564
(757) 444-1672 DSN: 564

UNCLAS FAX: (757) 444-3139 DSN: 564

AFTER HOURS:
DUTY TEXT NOTIFICATION: (757) 475-2481

NAVAL BASE:
POLICE WATCH CAPTAIN: (757) 322-2551

NCIS/NLETS ORI: VANIS0900
NMSG PLA: NAVCRIMINSVERFO NORFOLK VA//NFNF//
UIC: 45086

TERRITORIAL COVERAGE: ALL MILITARY INSTALLATIONS (SHORE AND AFLOATS) IN VIRGINIA, LESS THE COUNTIES OF: ARLINGTON, CAROLINE, CLARKE, CULPEPPER, ESSEX, FAIRFAX, FAUQUIER, FREDERICK, GREENE, KING GEORGE, LANCASTER, LOUDOUN, MADISON, NORTHCUMBERLAND, ORANGE, PAGE, PRINCE WILLIAM, RAPPAHANNOCK, RICHMOND COUNTY, ROCKINGHAM, SHENANDOAH, SPOTSYVANIA, STAFFORD, WARREN AND WESTMORELAND.

2356072 12:22 20160204 IN:SSDEMAIL #6 OUT:NCISWWSSD #4

GENERAL ADMINISTRATION 04FEB16

FROM: NFNF GEN: NF-0005

TO: DIST

SUBJ: NCIS - 2 (NFXO) NCISRU USS GEORGE WASHINGTON (CVN-73) DATA SHEET

ADCON: NFNF OPCON: NFNF

MAILING ADDRESS

ATTN: SAA - USS GEORGE WASHINGTON (CVN-73) NAVAL CRIMINAL INVESTIGATIVE SERVICE NORFOLK FIELD OFFICE
1329 BELLINGER BLVD
NORFOLK VA 23511-2310

NMSG PLA: NAVCRIMINVSERVREP XRAY OSCAR

UIC: 21412

FOR OFFICIAL USE ONLY
PAGE 1 LAST (b)(6)

2216105 17:14 20151214 IN:SSDEMAIL #19 OUT:NCISWWSSD #19

GENERAL ADMINISTRATION 14DEC15

FROM: NFNF GEN: NF-0044

TO: DIST

SUBJ: NCIS - 2 (NFYT) - NCISRU YORKTOWN DATA SHEET

PARENT NCISFO: NFFO
PARENT NCISRA: NFNF

NOTE: Until the Code of NFYT has been established in the Consolidated Law Enforcement Operations Center (CLEOC) around the end of January 2016, NCIS offices will use the office code of NFNF for sending leads to NCISRU Yorktown when using CLEOC.

LOCAL/MAILING ADDRESS

NCISRU YORKTOWN
2029 LONGFELLOW ROAD
NAVAL WEAPONS STATION
YORKTOWN, VA 23691-1900

TELEPHONE
OFFICE: COM - (757) 887-7305

UIC: 45188

TERRITORIAL COVERAGE: COUNTIES OF HANOVER, NEW KENT, YORK, HENRICO, CHESTERFIELD, JAMES CITY, GLOUCESTER, GOOCHLAND, POWHATAN, MIDDLESEX, MATTHEWS AND POQUOSON AND THE NEARBY CITIES OF RICHMOND, WILLIAMSBURG, HAMPTON AND NEWPORT NEWS.

2235609 08:35 20151222 IN:SSDEMAIL #1 OUT:NCISWWSSD #1

GENERAL ADMINISTRATION 22DEC15

FROM: 0022 GEN: 22-0015

TO: DIST

SUBJ: NCIS-2/NATIONAL SECURITY DIRECTORATE KEY PERSONNEL DATA SHEET (0022)

MAILING ADDRESS
NAVAL CRIMINAL INVESTIGATIVE SERVICE
HEADQUARTERS (NCISHQ CODE 0022)
27130 TELEGRAPH ROAD
QUANTICO, VA 22134

TELEPHONES
DSN PREFIX: INCOMING 240-XXXX (LAST 4)
OUTGOING 94-XXX-XXXX (CONUS)
OUTGOING 94-312-XXX-XXXX (OCONUS)
OFFICE: 571-305-9689 (TEMP)
UNCLASS FAX: 571-305-9574
SECURE FAX: (b)(6)

NAVMSG PLA: NAVCRIMINVSERVHQ NSD QUANTICO VA

CODE/PERSONNEL TELEPHONE NUMBERS

EXECUTIVE ASSISTANT DIRECTOR b6
VACANT CELL: XXX-XXX-XXXX

ASSISTANT DIRECTOR (b)(6)
(b)(6)

SENIOR POLICY ADVISOR (b)(6)
(b)(6)

STATE DEPARTMENT REPRESENTATIVE (b)(6)
(b)(6)

DEPUTY UNDER SECRETARY DEFENSE INTEL (b)(6)
(b)(6)

JOINT STAFF CCICA (b)(6)
(b)(6)

22A PROGRAM DIRECTION

DEPUTY ASSISTANT DIRECTOR (b)(6)
(b)(6)

SENIOR PROGRAM ANALYST (b)(6)
(b)(6)

FOR OFFICIAL USE ONLY
PAGE 1

22DEC15

SUBJ: NCIS-2/NATIONAL SECURITY DIRECTORATE KEY PERSONNEL DATA SHEET

DIVISION CHIEF (b)(6)
(b)(6)

SUPERVISORY SPECIAL AGENT PROGRAMS/POLICY (b)(6)
(b)(6)

FPD PROGRAM MANAGER OFFICE: (b)(6)
(b)(6)

FOSO (b)(6)
(b)(6)

22B INVESTIGATIONS

DEPUTY ASSISTANT DIRECTOR (b)(6)
(b)(6)

DIVISION CHIEF (b)(6)
(b)(6)

NCIS REP. TO NAVSEA 08 (Naval Reactors) (b)(6)
(b)(6)

SUPERVISORY SPECIAL AGENT INV (b)(6)
(b)(6)

DIVISION CHIEF INSIDER THREAT (b)(6)
(b)(6)

SUPERVISORY SPECIAL AGENT INSIDER THREAT (b)(6)
(b)(6)

LNO N2N6 (b)(6)
(b)(6)

NJTTF DEPUTY UNIT CHIEF (b)(6)
(b)(6)

STAFF PSYCHOLOGIST (b)(6)
(b)(6)

22C OPERATIONS

DEPUTY ASSISTANT DIRECTOR (b)(6)
(b)(6)

DIVISION CHIEF, IRREG/RDA WARFARE (b)(6)
(b)(6)

SUPERVISORY SPECIAL AGENT RDA (b)(6)
(b)(6)

22DEC15

SUBJ: NCIS-2/NATIONAL SECURITY DIRECTORATE KEY PERSONNEL DATA SHEET

DIVISION CHIEF, OPERATIONS (b)(6)
(b)(6)

SUPERVISORY SPECIAL AGENT OPS OFFICE: XXX-XXX-XXXX
VACANT CELL: XXX-XXX-XXXX

SR. NCIS REP, OUSN, DUSN (b)(6)
(b)(6)

DIVISION CHIEF, SENSITIVE PRO. INTIGRATION (b)(6)
(b)(6)

22D CYBER & DEFENSE CRITICAL INFRASTRUCTURE PROTECTION

DIVISION CHIEF PROGRAMS (b)(6)
(b)(6)

SUPERVISORY SPECIAL AGENT (b)(6)
(b)(6)

CYBER TECH PROGRAM MANAGER OFFICE: 571-305-XXXX
VACANT CELL: XXX-XXX-XXXX

COMPUTER LAW AND NATIONAL SECURITY (b)(6)
(b)(6)

NCIS REP TO CYBERCOM J2X (b)(6)
(b)(6)

NCIS REP TO FCC/C10F (b)(6)
(b)(6)

NCIS REP TO FBI NCIJTF (b)(6)
(b)(6)

22 ANALYTIC DIVISION

SUPERVISORY INTELLIGENCE SPECIALIST (b)(6)
(b)(6)

SUPERVISORY INTELLIGENCE SPECIALIST (b)(6)
(b)(6) CELL:

22 LEGAL DIVISION

FOR OFFICIAL USE ONLY
PAGE 3

22DEC15

SUBJ: NCIS-2/NATIONAL SECURITY DIRECTORATE KEY PERSONNEL DATA SHEET

NATIONAL SECURITY LAW (b)(6)
(b)(6)

FOR OFFICIAL USE ONLY
PAGE 4 LAST (b)(6)

2351619 12:08 20160203 IN:SSDEMAIL #4 OUT:NCISWWSSD #3

GENERAL ADMINISTRATION 03FEB16

FROM: NFNF GEN: NF-0002

TO: DIST

SUBJ: NCIS - 2 (NFNF) NCISRA NORFOLK VA DATA SHEET

PARENT NCISFO: NFFO

NOTE SUBORDINATE OFFICES: NFCE, NFFM, NFHV, NFLC, NFPV, NFYT, NFXA, NFXH, NFXL, NFXO, NFXQ, NFX1, NFX3

NOTE: NCIS OFFICES UNDER NCISRA NORFOLK ARE SERVICED BY THE NCIS CENTRAL EVIDENCE FACILITY (CEF) AND EVIDENCE SHOULD BE MAILED DIRECTLY TO THEM AT: 9079 HAMPTON BLVD, SUITE 110, NORFOLK VA 23505-1098. THE LONG TERM STORAGE (LTS) FACILITY IS STILL PENDING THE TESTING AND IMPLEMENTATION OF AN ELECTRONIC CUSTODY SYSTEM. FURTHER GUIDANCE IS PENDING.

MAILING ADDRESS LOCAL ADDRESS

NCIS NORFOLK FIELD OFFICE
1329 BELLINGER BLVD
NORFOLK VA 23511-2310

(b)(6)

TELEPHONES:

OFFICE: (757) 444-7327 DSN: 564
(757) 444-1672 DSN: 564

UNCLAS FAX: (757) 444-3139 DSN: 564

AFTER HOURS:
DUTY TEXT NOTIFICATION: (757) 475-2481

NAVAL BASE:
POLICE WATCH CAPTAIN: (757) 322-2551

NCIS/NLETS ORI: VANIS0900
NMSG PLA: NAVCRIMINSVERFO NORFOLK VA//NFNF//
UIC: 45086

TERRITORIAL COVERAGE: ALL MILITARY INSTALLATIONS (SHORE AND AFLOATS) IN VIRGINIA, LESS THE COUNTIES OF: ARLINGTON, CAROLINE, CLARKE, CULPEPPER, ESSEX, FAIRFAX, FAUQUIER, FREDERICK, GREENE, KING GEORGE, LANCASTER, LOUDOUN, MADISON, NORTHCUMBERLAND, ORANGE, PAGE, PRINCE WILLIAM, RAPPAHANNOCK, RICHMOND COUNTY, ROCKINGHAM, SHENANDOAH, SPOTSYVANIA, STAFFORD, WARREN AND WESTMORELAND.

FOR OFFICIAL USE ONLY
PAGE 1 LAST (b)(6)

1639738 13:19 20150508 IN:SSDEMAIL #1 OUT:NCISWWSSD #1

GENERAL ADMINISTRATION 08MAY15

FROM: 002G GEN: 2G-0002

TO: DIST

SUBJ: NCIS-1/OFFICE OF FORENSIC SUPPORT (OFS) KEY PERSONNEL LISTING

(b)(6)

MAILING AND LOCAL ADDRESS:
Naval Criminal Investigative Service
Office of Forensic Support: 2GFG
Russell-Knox Building
27130 Telegraph Road
Quantico, VA 22134

Vacant
Forensic Consultant
Office Code: 2GFJ
Coverage Area: SEFO, MEFO, CRFO
Mailing Address:
NCIS Southeast Field Office

(b)(6)

Coverage Areas: FEFO and SNFO
Office Code: 2GFK
Mailing Address:

(b)(6)

FOR OFFICIAL USE ONLY
PAGE 1

08MAY15

SUBJ: NCIS-1/OFFICE OF FORENSIC SUPPORT (OFS) KEY PERSONNEL LISTING

(b)(6)

Office Coverage: 2GFD
Coverage Area: MWFO
Mailing Address:
NCIS Marine Corps West Field Office
Bldg. 120101 De Luz Road
Camp Pendleton, CA 92055-5238

(b)(6)

Office Code: 2GFW
Coverage Areas: DCFO, NEFO, CRFO
Mailing Address:
NCIS Washington Field Office
2713 Mitscher Road, SW
Bldg. 168, STE 200
Anacostia Annex, DC 20373

(b)(6)

Coverage Areas: NWFO, CNFO
Office Code: 2GFS
Mailing Address:
NCIS Southwest San Diego Field Office
3405 Welles Street
Bldg. 57, STE 1
San Diego, CA 93136-5018

(b)(6)

Office Code: 2GFS
Coverage Area: SWFO
Mailing Address:
NCIS Southwest San Diego Field Office
3405 Welles Street
Bldg. 57, STE 1
San Diego, CA 93136-5018

08MAY15

SUBJ: NCIS-1/OFFICE OF FORENSIC SUPPORT (OFS) KEY PERSONNEL LISTING

(b)(6)

(b)(6)

Office Code: 2GFN
Coverage Areas: NFFO and EUFO
Mailing Address:
NCIS Norfolk Field Office
1329 Bellinger Boulevard
Norfolk, VA 23511

(b)(6)

Office Code: 2GFC
Coverage Areas: CAFO and MEFO
Mailing Address:
NCIS Carolinas Field Office
H32 Julian C. Smith Dr.
Camp Lejeune, NC 28547-1603

(b)(6)

Office Code: 2GFJ
Mailing Address:
NCIS Southeast Field Office
(b)(6)

(b)(6)

Office Code: 2GFL
Coverage Area: SEFO
Mailing Address:
US Army Criminal Investigation Laboratory (USACIL)
4930 N. 31st St, (b)(6)
Forest Park, GA 30297

Vacant
Forensic Consultant
Office Code: 2GFP
Coverage Area: CNFO

Mailing Address:
NCIS Central Field Office
(b)(6)

08MAY15

SUBJ: NCIS-1/OFFICE OF FORENSIC SUPPORT (OFS) KEY PERSONNEL LISTING

(b)(6)

(b)(6)

Office Code: 2GFI
Coverage Area: HIFO
Mailing Address:
NCIS Hawaii Field Office
449 South Ave
Bldg. 221
Pearl Harbor, HI 96860-4988

DISTRIBUTION
NCISHQ: All Departments and Directorates
INFO: WWSSD

FOR OFFICIAL USE ONLY
PAGE 4 LAST (b)(6)

1847657 13:35 20150722 IN:SSDEMAIL #8 OUT:NCISWWSSD #4

GENERAL ADMINISTRATION 22JUL15

FROM: 000C GEN: 00C-0038

TO: DIST

SUBJ: NCIS-2 (CODE 00C) COMMUNICATIONS DIRECTORATE DATA SHEET AND KEY PERSONNEL LISTING

PLEASE SEE THE BELOW FOR KEY PERSONNEL LISTING:

Director of Communications, (b)(6)
Office:
Blackb (b)(6)

Public Affairs Officer, (b)(6)
Offic
Cell: (b)(6)

Audiovisual Production Specialist, (b)(6)
Offic
Cell: (b)(6)

Writer/Editor, (b)(6)
Offic
Cell: (b)(6)

Website Content Manager, (b)(6)
Offic
Cell: (b)(6)

Graphic Specialist, (b)(6)
Offic
Cell: (b)(6)

Event Coordinator, (b)(6)
Offic
Cell: (b)(6)

Public Affairs Specialist, (b)(6) effective: 22JUL15)
Office: (b)(6)

Public Affairs Specialist, (b)(6) effective: 10AUG15)
Office: (b)(6)

FOR OFFICIAL USE ONLY
PAGE 1 LAST (b)(6)

1923793 09:35 20150819 IN:SSDEMAIL #1 OUT:NCISWWSSD #1

GENERAL ADMINISTRATION 18AUG15

FROM: 0000 GEN: 0I-0007

TO: DIST

SUBJ: NCIS-2/ (00I) OFFICE OF THE INSPECTOR GENERAL (00I) KEY PERSONNEL LISTING

MAILING ADDRESS/LOCAL ADDRESS
NAVAL CRIMINAL INVESTIGATIVE SERVICE HEADQUARTERS OFFICE OF INSPECTOR GENERAL ATTN: CODE 00I
27130 Telegraph Road W-3170
Quantico, VA 22134-2253

TELEPHONES COMMERCIAL
OFFICE: (571) 305-9O79
AFTER HOURS: NCIS MTAC (571) 305-4777

TITLE	KEY PERSONNEL
Inspector General	(b)(6)
Deputy IG	
Div Chief Investigations	
Div Chief Inspections	

SSA Vacant
Investigations

SSA Inspections

(b)(6)

FOR OFFICIAL USE ONLY
PAGE 1

18AUG15

SUBJ: NCIS-2/ (00I) OFFICE OF THE INSPECTOR GENERAL (00I) KEY PERSON

Investigative Assistant
Inspections Support

(b)(6)

Program Support Assistant
Admin Support

DISTRIBUTION
NCISHQ: All Directorates and Departments
INFO: WWSSD/AFLT

FOR OFFICIAL USE ONLY
PAGE 2 LAST (b)(6)

U.S. NAVAL CRIMINAL INVESTIGATIVE SERVICE

GENERAL ADMINISTRATION 31AUG15

FROM: OOSS GEN: OSS-0004

TO: DISTRIBUTION

SUBJ: NCIS-2 (OSS) OFFICE OF STRATEGIC SUPPORT DATA SHEET

MAILING ADDRESS:
NAVAL CRIMINAL INVESTIGATIVE SERVICE OFFICE OF STRATEGIC SUPPORT
2713 MITSCHER RD SW STE 300
JOINT BASE ANACOSTIA BOLLING DC 20373-5107

TELEPHONES	COMMERICAL	DSN
SAC	(b)(6)	
SSA		
SSA		

* DENOTES STU-III/STE CAPABILITY

UNCLAS//

FOR OFFICIAL USE ONLY

(b)(6)

WARNING

THIS DOCUMENT IS THE PROPERTY OF THE NAVAL CRIMINAL INVESTIGATIVE SERVICE CONTENTS MABY BE DISCLOSED ONLY TO PERSONS WHOSE OFFICIAL DUTIES REQUIRE ACCESS HERE TO CONTENTS MAY NOT BE DISCLOSED TO THE PARTY(S) CONCERNED WITHOUT SPECIFIC AUTHORIZATION FROM THE NAVAL CRIMINAL INVESTIGATIVE SERVICE

U.S. NAVAL CRIMINAL INVESTIGATIVE SERVICE

GENERAL ADMINISTRATION
31AUG15

FROM: OOSS

GEN: OSS-0005

TO: DISTRIBUTION

SUBJ: NCIS-2 (OSS) OFFICE OF STRATEGIC SUPPORT KEY PERSONNEL LISTING

MAILING ADDRESS:
NAVAL CRIMINAL INVESTIGATIVE SERVICE OFFICE OF STRATEGIC SUPPORT
12713 MITSCHER RD SW STE 300
JOINT BASE ANACOSTIA BOLLING, DC 20373-5107

(b)(6)

2. POC at OSS is (b)(6)

DISTRIBUTION
NCISHQ: ALL DEPARTMENT AND DIRECTORATES
INFO: WWSSD

FOR OFFICIAL USE ONLY

(b)(6)

WARNING

THIS DOCUMENT IS THE PROPERTY OF THE NAVAL CRIMINAL INVESTIGATIVE SERVICE CONTENTS MABY BE DISCLOSED ONLY TO PERSONS WHOSE OFFICIAL DUTIES REQUIRE ACCESS HERE TO CONTENTS MAY NOT BE DISCLOSED TO THE PARTY(S) CONCERNED WITHOUT SPECIFIC AUTHORIZATION FROM THE NAVAL CRIMINAL INVESTIGATIVE SERVICE

2302896 14:10 20160120 IN:SSDEMAIL #14 OUT:NCISWWSSD #6

GENERAL ADMINISTRATION 20JAN16

FROM: 2GTQ GEN: 02G-0002

TO: DIST

SUBJ: NCIS-2: OFFICE OF TECHNICAL SERVICES KEY PERSONNEL DATA SHEET

MAILING ADDRESS
Naval Criminal Investigative Service HQ
Office of Technical Services (OTS)(2GTQ) Russell-Knox Building
27130 Telegraph Road
Quantico, VA 22134-2253

TITLE/PERSONNEL CONTACT NUMBERS

(b)(6)

NCIS Norfolk Detachment (2GTV)
1801 Tomcat Blvd, Bldg 321
Virginia Beach, VA 23460-2289

(b)(6)

NCIS San Diego Detachment (2GTC)
3405 Welles Street
Bldg 57 Suite 1
San Diego, CA 92136

(b)(6)

(b)(6)

Field Operations Support Officer

(b)(6)

DISTRIBUTION

FOR OFFICIAL USE ONLY
PAGE 1

20JAN16

SUBJ: NCIS-2: OFFICE OF TECHNICAL SERVICES KEY PERSONNEL DATA SHEET

NCISHQ: All Departments and Directorates
INFO: WWSSD

2306077 08:13 20160121 IN:SSDEMAIL #1 OUT:NCISWWSSD #1

GENERAL ADMINISTRATION 21JAN16

FROM: 2GTQ GEN: 02G-0003

TO: DIST

SUBJ: NCIS-2: OFFICE OF TECHNICAL SERVICES DATA SHEET

MAILING ADDRESS
Naval Criminal Investigative Service HQ
Office of Technical Services Department (OTSD) Russell-Knox Building
27130 Telegraph Road
Quantico, VA 22134-2253

Telephones	Commercial	DSN
Office:	(571) 305-9177	240
Unclas Facsimile:	(571) 305-9085	
After Hours: NCIS MTAC	(571) 305-4777	

NMSG PLA: DIRNAVCRIMINVSERV Quantico VA/2GTQ// NCIC/NLETS ORI: None
UIC: 63285
Electrical Distribution: /2GTQ/

NCISTSD WASHINGTON (2GTS)
Co-Located With NCISHQ Code 2GTQ

Telephones	Commercial	DSN
Office:	(571) 305-9177	240
Unclas Facsimile:	(571) 305-9085	
After Hours: NCIS MTAC	(571) 305-4777	

Territorial Coverage:
District of Columbia; Virginia; Counties of Arlington; Fairfax, Loudoun, Accomack, Culpeper, Fauquier, Prince, William, Spotsylvania, Stafford, King George, Northampton, Westmoreland, Richmond, Lancaster, Essex, and Caroline, Orange, Green, Madison, Rockingham, Page, Rappahannock, Warren, Clarke, Frederick, and Shenandoah; Cities of Alexandria, Falls Church, Fairfax, Vienna, and Fredericksburg; State of Maryland.

DETACHMENTS:

NCISTSD Camp Lejeune (2GTD)
Mailing/Local Address
H-32 Julian C. Smith Drive
Camp Lejeune, NC 28547-1603

Telephones	Commercial	DSN
Office:	(910) 449-6516/4385	752
Unclas Facsimile:	(910) 449-6505	

FOR OFFICIAL USE ONLY

21JAN16

SUBJ: NCIS-2: OFFICE OF TECHNICAL SERVICES DATA SHEET

NCIC/NLETS ORI: NCNIS 0200
UIC: 35626 (CALE)

Territorial Coverage:
All Counties in North and South Carolina.

NCISTSD Hawaii (2GTH)
Mailing/Local Address
449 South Avenue
Pearl Harbor, HI 96860-4988

Local Address
(b)(6)

Telephones	Commercial	DSN
Office:	(808)447-0010/0021	315
Unclas Facsimile:	(808) 447-0025	

PLA: NAVCRIMINVSERV TECHSVC DET Pearl Harbor HI//2GTH// NCIC/NLETS ORI: None
UIC: 35630 (HIHN)

Territorial Coverage:
The State Of Hawaii (Including Oahu, Maui, Hawaii And Kauai Counties) Midway Island, Kingman Reef, Phoenix Islands, American Samoa, Baker Island, Cook Island, Daner Island, French Polynesia Islands, Howard Island, Johnston Island, Line Islands, Midway Island, Niue Island, Phoenix Islands, Pitcaim Islands, Tokelau Islands, Society Islands, Tuamotu Archipelago, Tubuai Islands, Western Samoa, Northern Marianas Islands, Federated States Of Micronesia, Republic Of Palau, Republic of the Marshall

Islands, Tokelau Islands, Society Islands, Tuamotu Archipelago, Marquesas Islands, Antarctica, Guam, Marianas Islands, Australia, New Zealand, Japan, Okinawa, Korea, Philippines, and Singapore.

NCISTSD Bahrain (2GTB)
Mailing/Local Address
PSC 851 Box 520
FPO AE 09834-0006

Local/Delivery Address (FEDEX,UPS,DHL)
(b)(6)
(b)(6)

Telephones	Commercial	DSN
Office:	011-973-1785-4392	318
Unclas Facsimile:	011-973-1785-4116	

Territorial Coverage:
The Middle East, Arabian Peninsula, Arabian Gulf, Gulf Of Aden, Gulf Of Oman, The Red Sea, and the Islands of Mauritius and Seychelles.

The Middle East Countries Specifically Covered Are:
Bahrain, Egypt, Iran, Jordan, Kazakhstan, Kuwait, Kyrgyzstan, Lebanon, Mauritius, Oman, Pakistan, Qatar, Saudi Arabia, Seychelles,

21JAN16

SUBJ: NCIS-2: OFFICE OF TECHNICAL SERVICES DATA SHEET

Syria, Tajikistan, Turkmenistan, United Arab Emirates, Uzbekistan, Yemen

NCISTSD Norfolk (2GTV)
Mailing/Local Address
1801 Tomcat Blvd
Bldg 321, Virginia Beach, VA 23460

Telephones	Commercial	DSN
Office:	(757) 433-3885	433
Unclas Facsimile:	(757) 433-3949	

PLA: NAVCRIMINVSERV TECH SVC DET Norfolk VA//2GTV//
UIC: 63055

Territorial Coverage: All Military Installations (Shore and Afloat) in Virginia, less the Counties of: Arlington, Caroline, Clarke, Culpeper, Essex, Fairfax, Fauquier, Frederick, Greene, King George, Lancaster, Loudoun, Madison, Northumberland, Orange, Page, Prince William, Rappahannock, Richmond, Rockingham, Shenandoah, Spotsylvania, Stafford, Warren and Westmoreland.

NCISTSD Bangor (2GTG)
Mailing/Local Address
1003 Sunfish Drive
Silverdale, WA 98315

Telephones	Commercial	DSN
Office:	(360) 396-4408/7195	744
Unclas Facsimile:	(360) 396-4424	

PLA: NAVCRIMINVSERV TECH SVC DET Bangor WA//2GTG//
UIC: 42951 (NWBG)

Territorial Coverage:
Alaska, California: All Counties, north of, and including, San Luis Obispo, King and Inyo. Washington, Oregon, Idaho, Montana, Utah, Colorado, Wyoming, Northern Nevada.

NCISTSD Jacksonville (2GTM)
Mailing Address
Po Box 58
Naval Air Station
Jacksonville, FL 32212-0058

Local/Delivery Address (FedEx, Ups)
(b)(6)
(b)(6)

Telephones	Commercial	DSN
Office:	(904) 542-2684/5369	542
Unclas Facsimile:	(904)542-8631	

NMSG PLA: DIRNAVCRIMINVSERVFO Southeast Mayport FL//2GTM// NCIC/NLETS ORI: None

21JAN16

SUBJ: NCIS-2: OFFICE OF TECHNICAL SERVICES DATA SHEET

UIC: 42933 (SEFO)

Territorial Coverage:
Providing Technical Support to the Southeast Field Office and parts of Gulf Coast Field Office. Areas Of Responsibility (AOR) include Alabama, Arkansas, Florida, Georgia, Louisiana, Mississippi, Oklahoma, Tennessee, and Texas. All Counties except El Paso, Hudspeth and Culberson; South America and the Caribbean.

NCISTSD San Diego (2GTC)
Mailing Address
3405 Welles Street
Bldg 57 Suite 1
San Diego, CA 92136

Telephones	Commercial	DSN
Office:	(619) 524-0613/0605	524
Unclas Facsimile:	(619) 524-0618	

NMSG PLA: DIRNAVCRIMINSERV TECHSVC DET San Diego CA//2GTC// NLETS/NCIC ORI: Caniso400
UIC: 42943

Territorial Coverage:
Arizona: All Counties
California: All Counties
Nevada: Clark Counties
New Mexico: All Counties
Oklahoma: All Counties
Texas: All Counties
El Paso: All Counties
Hudspeth: All Counties
Culberson: All Counties
South America and the Caribbean.

NCISTSD Europe and Africa
Mailing Address
PSC 812 Box 3360
FPO AE 09627-3360

Local Address

(b)(6)

Telephones	Commercial	DSN
From Conus:	011-39-095-86-9264	314
Within Italy:	095-86-9264	

Within Europe: 0039-095-86-9264

The above office is not manned on a continuous basis, please contact HQ if no one responds. 571-305-9177.

21JAN16

SUBJ: NCIS-2: OFFICE OF TECHNICAL SERVICES DATA SHEET

Note: For technical support for Europe/Africa AOR please send leads to NCISHQ Code 2GTQ.

Territorial Coverage: Continent of Europe and all Littoral Areas, United Kingdom, Iceland, Turkey and Israel. Continent of Africa (except for Egypt and the Islands of Seychelles and Mauritius).

FOR OFFICIAL USE ONLY
PAGE 5 LAST (b)(6)

2214538 11:51 20151214 IN:SSDEMAIL #16 OUT:NCISWWSSD #16

GENERAL ADMINISTRATION 14DEC15

FROM: SEFO GEN: SE-0032

TO: DIST

SUBJ: 53342035MH.DOC - *CORRECTED COPY* NCIS-2 (SEAU/CNAU) NCISRU
AUSTIN TX DATA SHEET

**********CI COVERAGE ONLY**********

PARENT NCISFO: SOUTHEAST FIELD OFFICE MAYPORT FL (SEFO) PARENT NCISRA: PENSACOLA FL (SEPF/CNPF)

NOTE: NCISRU AUSTIN TX is no longer under the ADCON/OPCON of Central Field Office as of 01NOV15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNAU, assigned to NCISRU AUSTIN TX, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code SEAU/NCISRU AUSTIN TX will not be used until NJIS comes online. Please copy SEFO/CNPF, as appropriate. All other correspondence will utilize SEAU.

MAILING ADDRESS AND LOCAL ADDRESS:
FEDERAL BUREAU OF INVESTIGATION
TFO TROY NOBLE, CI-2
12515-7 RESEARCH BLVD FBI
SUITE 400 SUITE 400
AUSTIN, TX 78759 AUSTIN, TX 78759

TELEPHONES COMMERCIAL ONLY
OFFICE 512-506-4111
CELL PHONE 512-731-4719
UNCLAS FAX 512-506-2686 (USE COVER SHEET)

SSD TELECOMMS
NMSG PLA: NAVCRIMINVSERVRA AUSTIN TX
NCIC/NLET ORI: NONE
UIC: N34416

TERRITORIAL COVERAGE: CI/RTP/CE LEADS ONLY. ALL GENCRIM/FRAUD/CBT LEADS SHOULD BE DIRECTED TO SECC/CNCC, SESO/CNSO, OR SEDA/CNDA (SEE NCIS 2 FOR AOR).

TEXAS: ALL COUNTIES EXCEPT FOR EL PASO, HUDSPETH, REEVES AND CULBERTSON.
OKLAHOMA: ALL COUNTIES
KANSAS: ALL COUNTIES
PRINCIPAL INSTALLATION SERVICED:
UNIVERSITY OF TEXAS, APPLIED RESEARCH LABORATORY, AUSTIN, TX

**********CI COVERAGE ONLY**********

FOR OFFICIAL USE ONLY
PAGE 1 LAST (b)(6)

2214363 10:47 20151214 IN:SSDEMAIL #11 OUT:NCISWWSSD #11

GENERAL ADMINISTRATION 14DEC15

FROM: SEFO GEN: SE-0024

TO: DIST

SUBJ: NCIS-2 (SECC/CNCC) NCISRU CORPUS CHRISTI TX DATA SHEET

PARENT NCISFO: SOUTHEAST FIELD OFFICE (SEFO) PARENT NCISRA: DALLAS TX (SEDA/CNDA)

NOTE: NCISRU CORPUS CHRISTI TX is no longer under the ADCON/OPCON control of Central Field Office as of 01NOV15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNCC, assigned to NCISRU CORPUS CHRISTI TX, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code SECC/NCISRU CORPUS CHRISTI TX will not be used until NJIS comes online. Please copy SEFO/CNDA, as appropriate. All other correspondence will utilize SECC.

MAILING ADDRESS	LOCAL ADDRESS
385 FIFTH ST SE SUITE 2A	BUILDING 39
CORPUS CHRISTI, TX 78419-5034	NAVAL AIR STATION
	CORPUS CHRISTI TX 78419-5034

TELEPHONES	COMMERCIAL	DSN PREFIX
OFFICE	(361) 961-2918/2919/2839	861
UNCLAS FAX	(361) 961-2429	861
SECURE FAX	(b)(6)	

(b)(6)

SSD TELECOMMUNICATIONS: NIPRNET
NMSG PLA: NAVCRIMINVSERVREP CORPUS CHRISTI TX NCIC/NLET ORI: NONE
UIC: 42936
BASE STATION IDENTIFIER CODE (NFC): 1181

TERRITORIAL COVERAGE:
THE FOLLOWING COUNTIES: ANGELINA; ARANSAS; AUSTIN; BEE; BROOKS; BRAZORIA; BURLESON; CALHOUN; CAMERON; CHAMBERS; COLORADO; DEWITT; DUVAL; FORT BEND; GALVESTON; GOLIAD; GRIMES; HARDIN; HARRIS; HILDALGO; HOUSTON; JACKSON; JASPER; JEFFERSON; JIM HOGG; JIM WELLS; LIVE OAK; KENEDY; KLEBERG; LIBERTY; MATAGORDA; MCMULLEN; MONTGOMERY; NEWTON; NUECES;

ORANGE; POLK; REFUGIO; SAN JACINTO; SAN PATRICIO; TRINITY; TYLER; VICTORIA; WALKER; WALLER; WHARTON; WILLACY;

PRINCIPAL INSTALLATION SERVICED:
CNATRA NAS KINGSVILLE NOSC HARLINGEN
TRAWING TWO NAS CORPUS CHRISTI NOSC CORPUS CHRISTI TRAWING FOUR MATSG CORPUS CHRISTI
VT-21 MCRD HOUSTONVT-22 NRD HOUSTON

FOR OFFICIAL USE ONLY
PAGE 1

14DEC15

SUBJ: NCIS-2 (SECC/CNCC) NCISRU CORPUS CHRISTI TX DATA SHEET

VT-27 PSA CORPUS CHRISTI
VT-28 NAVRESCEN HOUSTON
VT-31 NAVRESCEN CORPUS CHRISTI
VT-35 PSA CORPUS CHRISTI

FOR OFFICIAL USE ONLY
PAGE 2 LAST (b)(6)

2224330 08:23 20151217 IN:SSDEMAIL #1 OUT:NCISWWSSD #1

GENERAL ADMINISTRATION 17DEC15

FROM: SEFO GEN: SE-0035

TO: DIST

SUBJ: *CORRECTED COPY" NCIS-2 (SEDA/CNDA) NCISRA DALLAS TX DATA SHEET

PARENT NCISFO: SOUTHEAST FIELD OFFICE MAYPORT FL (SEFO) SUBORDINATE NCISRU: SESO/CNSO, SECC/CNCC, SEOC/CNOC

NOTE: NCISRA DALLAS TX is no longer under the ADCON/OPCON control of Central Field Office as of 01NOV15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNDA, assigned to NCISRA DALLAS TX, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code SEDA/NCISRA DALLAS TX will not be used until NJIS comes online. Please copy SEFO, as appropriate. All other correspondence will utilize SEDA.

MAILING AND LOCAL ADDRESS
1701 E. LAMAR BLVD STE 292
ARLINGTON, TX 76011

TELEPHONES COMMERCIAL ONLY
OFFICE (817) 860-5260
UNCLAS FAX (817) 860-2394
AFTER HOURS NAS JRB FORT WORTH, TX (817) 782-5200 SECURITY DISPATCH

DMS PLA: NAVCRIMINVSERVRA DALLAS TX
NCIS-CNFO ORI: ILNIS1000
UIC: 34415

TERRITORIAL COVERAGE
THE FOLLOWING COUNTIES: ANDERSON; ANDREWS; ARCHER; ARMSTRONG; BAILEY; BAYLOR; BELL; BORDEN; BOSQUE; BOWIE; BRAZOS; BRISCOE; BROWN; CALLAHAN; CAMP; CARSON; CASS; CASTRO; CHEROKEE; CHILDRESS; CLAY; COCHRAN; COKE; COLEMAN; COLLIN; COLLINGSWORTH; COMANCHE; CONCHO; COOKE; CORYELL; COTTLE; CRANE; CROSBY; DALLUM; DALLAS; DAWSON; DEAF SMITH; DELTA; DENTON; DICKINS; DONLEY; EASTLAND; ECTOR; ELLIS; ERATH; FALLS; FANNIN; FISHER; FLOYD; FOARD; FRANKLIN; FREESTONE; GAINES; GARZA; GLASSOCK; GRAY; GRAYSON; GREGG; HALE; HALL; HAMILTON;

HANSFORD; HARDEMAN; HARRISON; HARTLEY; HASKELL; HEMPHILL; HENDERSON; HILL; HOCKLEY; HOOD; HOPKINS; HOWARD; HUNT; HUTCHINSON; JACK; JOHNSON; JONES; KAUFMAN; KENT; KING; KNOX; LAMAR; LAMB;LAMPASAS; LEON; LYPSCOMB; LIMESTONE; LUBBOCK; LOVING; LYNN; MCCLENNAN; MADISON; MARION; MARTIN; MIDLAND; MILLS; MITCHELL; MONTAGUE; MOORE; MORRIS; MOTLEY; NACOGDOCHES; NAVARRO; NOLAN; OCHILTREE; OLDHAM; PALO PINTO; PANOLA; PARKER; PARMER; POTTER; RAINS; RANDALL; RED RIVER; !
REEVES; ROBERTS; ROCKWALL; RUNNELS; RUSK; SABINE; SAN AUGUSTINE; SCURRY; SHACKELFORD; SHELBY; SHERMAN; SMITH; SOMERVELL; STEPHENS;

FOR OFFICIAL USE ONLY
PAGE 1

17DEC15

SUBJ: *CORRECTED COPY" NCIS-2 (SEDA/CNDA) NCISRA DALLAS TX DATA SHEE

STERLING; STONEWALL; SWISHER; TARRANT; TAYLOR; TERRY; THROCKMORTON; TITUS; TOM GREEN; UPSHUR; VAN ZANDT; WARD; WHEELER; WINKLER; WITCHITA; WILBARGER; WISE; WOOD; YOAKUM; YOUNG;

PRINCIPAL INSTALLATIONS SERVICED
NAS JRB FT WORTH 8TH MARINE RECRUITING DISTRICT 14TH MARREG NAVCRUITDIST DALLAS
COMFLELOGSUPPWING NAVPRO DALLAS COMNAVRESINTEL COMM NORTHRUP/GRUMMAN AIRCORP
NOCD DALLAS DCMA DALLAS REGION VMFA-112
VR-59 VR-6
MAG-41 NAVAL OPERATION SUPPORT CENTER (NOSC)
MACS-24 FLEET READINESS CENTER (FRC) WEST
MWSS-473 BRANCH MEDICAL CLINIC

FOR OFFICIAL USE ONLY
PAGE 2 LAST (b)(6)

2214379 10:52 20151214 IN:SSDEMAIL #13 OUT:NCISWWSSD #13

GENERAL ADMINISTRATION 14DEC15

FROM: SEFO GEN: SE-0029

TO: DIST

SUBJ: NCIS-2 (SEGF/CNGF) NCISRA GULFPORT MS DATA SHEET

PARENT NCISFO: SOUTHEAST FIELD OFFICE MAYPORT FL (SEFO) SUBORDINATE NCISRU: MERIDIAN (SEMJ/CNMJ), NEW ORLEANS (SENR/CNNR)

NOTE: NCISRA GULFPORT MS is no longer under the ADCON/OPCON control of Central Field Office as of 01OCT15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNGF, assigned to NCISRA GULFPORT MS, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code SEGF/NCISRA GULFPORT MS will not be used until NJIS comes online. Please copy SEFO/CNPF, as appropriate. All other correspondence will utilize SEGF.

MAILING AND LOCAL ADDRESS
NCBC BLDG 109
2208 BARRY AVENUE
GULFPORT MS 39501

TELEPHONES	COMMERCIAL	DSN PREFIX
OFFICE	(228) 871-2211	868
UNCLAS FAX	(228) 871-3068	868
AFTER HOURS SECURITY	(228) 871-2361	868

NMSG PLA: NAVCRIMINVSERVRA GULFPORT MS
NCIC/NLETS ORI: NONE
UIC: 34413

TERRITORIAL COVERAGE:
MISSISSIPPI - THE FOLLOWING COUNTIES:
HARRISON, HANCOCK, JACKSON, PEARL RIVER, STONE, GEORGE, GREENE, PERRY, FORREST, LAMAR, MARION, WALTHALL, PIKE, AMITE, WILKINSON, ADAMS, FRANKLIN, LINCOLN, LAWRENCE, JEFFERSON DAVIS, COVINGTON, JONES, WAYNE, CLARKE, JASPER, SMITH SIMPSON, COPIAH, JEFFERSON, AND CLAIBORNE

ALABAMA - THE FOLLOWING COUNTIES:
MOBILE, WASHINGTON, CLARKE, CHOCTAW, MARENGO, SUMTER, GREENE, AND HALE

PRINCIPAL INSTALLATIONS SERVICED:
CBC GULFPORT; RESERVE NAVAL CONSTRUCTION FORCE; NCG2; NAVAGATIONAL AIDS SUPPORT UNIT; NMCB-1; NMCB-11; NMCB 74; NMCB 133; INSPECTOR-INSTRUCTOR STAFF (USMC); STENNIS SPACE CENTER, NAVOCEANO; NAVAL RESEARCH LABORATORY DETACHMENT; COMNAVOCEANCOM; AVOCEANOCOMFAC; SPECIAL BOAT UNIT TWENTY-TWO; CHIEF OF NAVAL METEOROLOGICAL AND OCEANOGRAPHY COMMAND (CNMOC); NAVAL OCEANOGRAPHY ASW CENTER; NAVAL

14DEC15

SUBJ: NCIS-2 (SEGF/CNGF) NCISRA GULFPORT MS DATA SHEET

SMALL CRAFT INSTRUCTION AND TECHNICAL TRAINING SCHOOL (NAVSCIATTS); NAVAL FLEET SURVEY TEAM; NAVAL METEOROLOGY AND OCEANOGRAPHY PROFESSIONAL DEVELOPMENT CENTER (PDC) SOUTH; NAVY HUMAN RESOURCES SERVICE CENTER SOUTHEAST.

FOR OFFICIAL USE ONLY
PAGE 2 LAST (b)(6)

2214391 10:55 20151214 IN:SSDEMAIL #15 OUT:NCISWWSSD #15

GENERAL ADMINISTRATION 14DEC15

FROM: SEFO GEN: SE-0031

TO: DIST

SUBJ: NCIS-2 (SEMJ/CNMJ) NCISRU MERIDIAN MS DATA SHEET

PARENT NCISFO: SOUTHEAST FIELD OFFICE MAYPORT FL (SEFO) PARENT NCISRA: GULFPORT MS (SEGF/CNGF)

NOTE: NCISRU MERIDIAN MS is no longer under the ADCON/OPCON of Central Field Office as of 01OCT15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNMJ, assigned to NCISRU MERIDIAN MS, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code SEMJ/NCISRU MERIDIAN MS will not be used until NJIS comes online. Please copy SEFO/CNPF, as appropriate. All other correspondence will utilize SEMJ.

MAILING AND LOCAL ADDRESS
NCISRU MERIDIAN
255 ROSENBAUM AVENUE
ROOM 134
MERIDIAN MS 39309

TELEPHONES	COMMERCIAL	DSN PREFIX
OFFICE	(601) 679-2564	637
UNCLAS FAX	(601) 679-2060	637
AFTER HOURS SECURITY	(601) 679-2361	637

DMS PLA: NAVCRIMINVSERVRA GULFPORT MS
NCIC/NLETS ORI: NONE
UIC: 67980

TERRITORIAL COVERAGE:
MISSISSIPPI: ALL COUNTIES NORTH OF INTERSTATE 20:
WARREN, HINDS, RANKIN, SCOTT, NEWTON, LAUDERDALE, KEMPER, NESHOBA, LEAKE, MADISON, YAZOO, SHARKEY, ISSAQUENA, WASHINGTON, HUMPHREYS, HOLMES, ATTALA, WINSTON, NOXUBEE, LOWNDES, OKTIBBEHA, CHOCTAW, MONTGOMERY, CARROLL, LEFLORE, SUNFLOWER, BOLIVAR, TALLAHATCHIE, GRENEDA, WEBSTER, CLAY MONROE, CHICKASAW, CALHOUN, YALOBUSHA, COAHOMA, QUITMAN, PANOLA, LAFAYETTE, UNION, PONTOTOC, LEE, ITAWAMBA, TISHOMINGO, PRENTISS, ALCORN, TIPPAH, BENTON, MARSHALL, TATE, TUNICA AND DESOTO.

ALABAMA: THE FOLLOWING COUNTIES:

PICKENS, TUSCALOOSA, JEFFERSON, ST. CLAIR, CALHOUN, CLEBURNE, CHEROKEE, ETOWAH, BLOUNT, WALKER, FAYETTE, LAMAR, MARION, WINSTON, CULLMAN, FRANKLIN, COLBERT, LAUDERDALE, LAWRENCE, MORGAN, LIMESTONE, MADISON, JACKSON, MARSHALL AND DEKALB

PRINCIPAL INSTALLATIONS SERVICED:

14DEC15

SUBJ: NCIS-2 (SEMJ/CNMJ) NCISRU MERIDIAN MS DATA SHEET

NAS MERIDIAN, TRAINING AIR WING ONE, NTTC, MATSS-1, NOSC, FAA, CNATRA DETACHMENT MERIDIAN, NAFC

FOR OFFICIAL USE ONLY
PAGE 2 LAST (b)(6)

2214240 10:23 20151214 IN:SSDEMAIL #3 OUT:NCISWWSSD #3

GENERAL ADMINISTRATION 14DEC15

FROM: SEFO GEN: SE-0028

TO: DIST

SUBJ: NCIS-2 (SEMT/CNMT) NCISRU MEMPHIS DATA SHEET

PARENT NCISFO: SOUTHEAST FIELD OFFICE MAYPORT FL (SEFO) PARENT NCISRA: ST LOUIS MO (SESL/CNSL)

NOTE: NCISRU MEMPHIS TN is no longer under the ADCON/OPCON control of Central Field Office as of 01NOV15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNMT, assigned to NCISRU MEMPHIS TN, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code SEMT/NCISRU MEMPHIS TN will not be used until NJIS comes online. Please copy SEFO/CNSL, as appropriate. All other correspondence will utilize SEMT.

MAILING ADDRESS	LOCAL ADDRESS (USE FOR FEDEX/UPS)
NCISRU MEMPHIS	NCISRU MEMPHIS
5722 INTEGRITY DRIVE	(b)(6)
MILLINGTON, TN 38054-5058	(b)(6)
	(b)(6)

TELEPHONES	COMMERCIAL	DSN
OFFICE:	(901)874-5387/89	882-5387
UNCLAS FAX:	(901)874-5218	882-5218
FCI STE:	(901)874-6247	882-6247

AFTER HOURS (SECURITY): (901)832-6177 (WATCH COMMANDER)

NMSG PLA: NAVCRIMINVSERVREP MEMPHIS TN
NCIC/NLETS ORI: NONE
UIC: 42937
BASE STATION IDENTIFIER CODE: NFC 656

TERRITORIAL COVERAGE
TENNESSEE - ALL COUNTIES
ARKANSAS - ALL COUNTIES

PRINCIPAL INSTALLATIONS SERVICED:
NAVY PERSONNEL COMMAND (NPC); NAVY RECRUITING COMMAND (NRC); NSA MID-SOUTH; DECA COMSY MEMPHIS, TN; NBHC MID-SOUTH; DPRO; MWRTU (WASHINGTON); NAVCRUITDIST MEMPHIS, TN; NAVMAC MEMPHIS, TN; PERSUPP DET MEMPHIS, TN; US AIR FORCE DET 2/CC (361TRS); USN & MCRTC KNOXVILLE, TN; NOSC MILLINGTON, TN; NOSC NASHVILLE, TN; NOSC KNOXVILLE, TN; NOSC CHATTANOOGA, TN; NOSC LITTLEROCK, AR.

2214382 10:53 20151214 IN:SSDEMAIL #14 OUT:NCISWWSSD #14

GENERAL ADMINISTRATION 14DEC15

FROM: SEFO GEN: SE-0030

TO: DIST

SUBJ: NCIS-2 (SENR/CNNR) NCISRU NEW ORLEANS LA DATA SHEET

PARENT NCISFO: SOUTHEAST FILED OFFICE MAYPORT FL (SEFO) PARENT NCISRA: GULFPORT MS (SEGF/CNGF)

NOTE: NCISRU NEW ORLEANS LA is no longer under the ADCON/OPCON of Central Field Office as of 01OCT15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNNR, assigned to NCISRU NEW ORLEANS LA, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code SENR/NCISRU NEW ORLEANS LA will not be used until NJIS comes online. Please copy SEFO/CNGF, as appropriate. All other correspondence will use SENR.

MAILING AND LOCAL ADDRESS
400 RUSSELL AVE
BLDG 557
NEW ORLEANS LA 70143

TELEPHONES	COMMERCIAL	DSN PREFIX
OFFICE	(504) 678-2257	678
UNCLAS FAX	(504) 678-3968	678
AFTER HOURS SECURITY	(504) 678-3333	678

DMS PLA: NAVCRIMINVSERVREP NEW ORLEANS LA NCIC/NLET ORI: NONE BASE STATION IDENTIFIER CODE: NFC 650
UIC: 42938

TERRITORIAL COVERAGE:
LOUISIANA: ALL PARISHES

PRINCIPAL INSTALLATIONS SERVICED: CG MARINE FORCES RESERVES; CG FOURTH MARINE AIR WING; CG FOURTH MARINE DIVISION; GC FOURTH MARINE LOGISTICS GROUP; MILITARY ENTRANCE PROCESSING STATION NEW ORLEANS; MILITARY SEALIFT COMMAND SURGE DETACHMENT NEW ORLEANS; NAVY AIR LOGISTICS OFFICE, NAVY RECRUITING DISTRICT NEW ORLEANS; NAVAL

AMBULATORY CARE CENTER NEW ORLEANS; NAVY RESERVE PROFESSIONAL DEVELOPMENT CENTER NEW ORLEANS; NAVY BAND NEW ORLEANS; NAVSUPPACT NEW ORLEANS; SUPSHIP GULF COAST NEW ORLEANS; SPAWARSYSCEN NEW ORLEANS; NAS JRB NEW ORLEANS; FLEET READINESS CENTER MID-ATLANTIC SITE NEW ORLEANS; NAVAL OPERATIONAL SUPPORT CENTER NEW ORLEANS; STRIKE FIGHTER SQUADRON 204 (VFA-204) NEW ORLEANS; FLEET LOGISTICAL SUPPORT SQUADRON 54 (VR-54) NEW ORLEANS; AIRBORN EARLY MORNING SQUAD (VAW-77) NEW ORLEANS; MARINE AIRCRAFT GROUP 49; DETACHMENT C NEW ORLEANS; 3RD BATTALION 23RD MARINES 4TH MARDIV NEW ORLEANS; NAVY AIR LOGISTIC

14DEC15

SUBJ: NCIS-2 (SENR/CNNR) NCISRU NEW ORLEANS LA DATA SHEET

OFFICE NEW ORLEANS

FOR OFFICIAL USE ONLY
PAGE 2 LAST (b)(6)

2214374 10:50 20151214 IN:SSDEMAIL #12 OUT:NCISWWSSD #12

GENERAL ADMINISTRATION 14DEC15

FROM: SEFO GEN: SE-0026

TO: DIST

SUBJ: NCIS-2 (SEOC/CNOC) NCISRU OKLAHOMA CITY OK DATA SHEET

PARENT NCISFO: SEFO
PARENT NCISRA: SEDA/CNDA

NOTE: NCISRU OKLAHOMA CITY OK is no longer under the ADCON/OPCON control of Central Field Office as of 01NOV15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNOC, assigned to NCISRU OKLAHOMA CITY OK, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code SEOC/NCISRU OKLAHOMA CITY OK will not be used until NJIS comes online. Please copy SEFO/CNDA, as appropriate. All other correspondence will utilize SECC.

MAILING AND LOCAL ADDRESS
AFOSI DET 114 TINKER AFB OK
ATTN: NCIS
3540 C AVENUE, BLDG 3
TINKER AFB, OK 73145-9114

TELEPHONES	COMMERCIAL	DSN
OFFICE:	202-421-0518	NONE
RESIDENT AGENT	202-421-0518	

DMAS PLA: NAVCRIMINVSERVRA DALLAS TX
NCIC/NLETS ORI: NONE
UIC: 34486

TERRITORIAL COVERAGE:
OKLAHOMA (ALL COUNTIES)
KANSAS (ALL COUNTIES)

PRINCIPAL INSTALLATIONS SERVICED:
CNAT; VQ-3; VQ-4; VQ-7

2214247 10:28 20151214 IN:SSDEMAIL #4 OUT:NCISWWSSD #4

GENERAL ADMINISTRATION 14DEC15

FROM: SEFO GEN: SE-0019

TO: DIST

SUBJ: NCIS-2 (SEPA/CNPA) NCISRU PASCAGOULA MS DATA SHEET

PARENT NCISFO: SOUTHEAST FIELD OFFICE MAYPORT FL (SEFO) PARENT NCISRA: JACKSONVILLE FL (SEJX - FRAUD)

NOTE: NCISRU PASCAGOULA MS is no longer under the ADCON/OPCON of Central Field Office as of 01OCT15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNPA, assigned to NCISRU PASCAGOULA MS, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code SEPA/NCISRU PASCAGOULA MS will not be used until NJIS comes online. Please copy SEFO/SEJX, as appropriate. All other correspondence will utilize SEPA.

MAILING ADDRESS: LOCAL ADDRESS
PO BOX 1652 535 DELMAS AVE STE 23
PASCAGOULA MS 39568-1652 PASCAGOULA MS 39567

TELEPHONES COMMERCIAL DSN
OFFICE (228) 769-4455 457-4455
UNCLAS FAX (228) 769-2743 457-2743
AFTER HOURS SECURITY (228) 871-2361 868-2361

DMS PLA: NAVCRIMINVSERVREP PASCAGOULA MS NCIC/NLETS ORI: NONE
UIC: 34414

TERRITORIAL COVERAGE:
ONLY MAJOR PROCUREMENT FRAUD INVESTIGATIONS/LEAD COVERAGE IN THE STATES OF MISSISSIPPI AND ALABAMA.

MISSISSIPPI: ALL COUNTIES

ALABAMA: MOBILE COUNTY AND ALL COUNTIES SOUTH OF INTERSTATE 20 EXCEPT BARBOUR, COFFEE, COVINGTON, CRENSHAW, DALE, GENEVA, HENRY, HOUSTON AND PIKE.

PRINCIPAL INSTALLATIONS SERVICED:
SUPSHIP GULF COAST PASCAGOULA, MS; INGALLS SHIPBUILDING PASCAGOULA, MS; BAE SHIPBUILDING, MOBILE, AL; AUSTAL SHIPBUILDING, MOBILE, AL; LITTORAL COMBAT SHIP PRECOMM UNITS AUSTAL USA MOBILE, AL.

2214267 10:37 20151214 IN:SSDEMAIL #7 OUT:NCISWWSSD #7

GENERAL ADMINISTRATION 14DEC15

FROM: SEFO GEN: SE-0022

TO: DIST

SUBJ: NCIS-2 (SEPC/CNPC) NCISRU PANAMA CITY FL DATA SHEET

PARENT NCISFO: SOUTHEAST FIELD OFFICE MAYPORT FL (SEFO) PARENT NCISRA: NCISRA PENSACOLA FL (SEPF/CNPF)

NOTE: NCISRU PANAMA CITY FL is no longer under the ADCON/OPCON of Central Field Office as of 01OCT15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNPC, assigned to NCISRU PANAMA CITY FL, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code SEPC/NCISRU PANAMA CITY FL will not be used until NJIS comes online. Please copy SEFO/CNPF, as appropriate. All other correspondence will utilize SEPC.

MAILING ADDRESS LOCAL ADDRESS
NAVAL SUPPORT ACTIVITY NAVAL SUPPORT ACTIVITY
101 VERNON AVE. BLDG 304 BLDG 304, ROOM 124
PANAMA CITY BEACH, FL 32407-7018

TELEPHONES COMMERCIAL DSN
OFFICE (850) 234-4306 436-4306/5695
UNCLAS FAX (850) 234-4857 436-4857
SECURE PHONE b7E
AFTER HOURS (SECURITY) (850) 234-4332 436-4332

NMSG PLA: NAVCRIMINVSERVREP PANAMA CITY FL NCIC/NLET ORI: NONE
UIC: 34412

TERRITORIAL COVERAGE
ALABAMA: COUNTIES OF BARBOUR, COFFEE, COVINGTON, CRENSHAW, DALE, GENEVA, HENRY, HOUSTON, PIKE, RUSSELL

FLORIDA: COUNTIES OF BAY, CALHOUN, FRANKLIN, GADSEN, GULF, HOLMES, JACKSON, LIBERTY, WAKULLA, WALTON AND WASHINGTON

PRINCIPAL INSTALLATIONS SERVICED:
NAVAL SUPPORT ACTIVITY PANAMA CITY, NAVAL SURFACE WARFARE CENTER NSWC), PANAMA CITY, NAVY EXPERIMENTAL DIVING UNIT (NEDU), CENTER FOR EOD AND DIVING, NAVY DIVING AND SALVAGE

TRAINING CENTER (NDSTC), EOD GROUP TWO DETACHMENT, FSD NROTC FLORIDA A&M UNIVERSITY, TALLAHASSEE, NAVRESCEN TALLAHASSEE

FOR OFFICIAL USE ONLY
PAGE 1 LAST (b)(6)

2221650 10:57 20151216 IN:SSDEMAIL #2 OUT:NCISWWSSD #2

GENERAL ADMINISTRATION 16DEC15

FROM: SEFO GEN: SE-0034

TO: DIST

SUBJ: *CORRECTED COPY* NCIS-2 (SEPF/CNPF) NCISRA PENSACOLA FL DATA SHEET

PARENT NCISFO: SOUTHEAST FIELD OFFICE MAYPORT FL (SEFO) SUBORDINATE NCISRU: AUSTIN TX (SEAU/CNAU); PANAMA CITY FL (SEPC/CNPC); FPD COLOMBIA (SECB); FPD HONDURAS (SETH); FPD GUATEMALA (SEGG)/ FPD EL SALVADOR (SESS)

NOTE: NCISRA PENSACOLA FL is no longer under the ADCON/OPCON of Central Field Office as of 01OCT15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNPF, assigned to NCISRA PENSACOLA FL, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code SEPF/NCISRA PENSACOLA FL will not be used until NJIS comes online. Please copy SEFO, as appropriate. All other correspondence will utilize SEPF.

NCISRA MAILING ADDRESS
821 SAN CARLOS ROAD
BUILDING 3813
NAVAL AIR STATION
PENSACOLA FL 32508-5133

LOCAL ADDRESS (CRIM/CT)
821 SAN CARLOS ROAD
BUILDING 3813
NAVAL AIR STATION
PENSACOLA FL 32508-5133

LOCAL ADDRESS (CI)
(b)(6)

TELEPHONES	COMMERCIAL	DSN PREFIX
OFFICE (CRIM/CT)	(850) 452-4211	459
OFFICE (CI)	(850) 452-6081	459
UNCLAS FAX (CRIM/CT)	(850) 452-4282	459
UNCLAS FAX (CI)	(850) 452-6193	459

(b)(6)

SSA (CRIM/CT/CI) (850) 452-4211 459
AFTER HOURS - DUTY AGENT VIA NAS SECURITY DEPT
(850) 452-3453/2453 459

NMSG PLA: NAVCRIMINVSERVRA PENSACOLA FL NCIC/NLETS ORI: ILNIS1020
UIC: 67556

TERRITORIAL COVERAGE
ALL ALABAMA COUNTIES FOR CRIM AND CI/CT

FOR OFFICIAL USE ONLY
PAGE 1

16DEC15

SUBJ: *CORRECTED COPY* NCIS-2 (SEPF/CNPF) NCISRA PENSACOLA FL DATA S

PRINCIPLE INSTALLATIONS SERVED:
NAS PENSACOLA; NAVAL AEROSPACE MEDICAL INSTITUTE (NAMI);NAVAL AEROSPACE MEDICAL RESEARCH LABORATORY (NAMRL); NAVAL AIR TECHNICAL TRAINING CENTER (NATTC); MARINE AVIATION TRAINING SUPPORT GROUP 21 (MATSG-21); NAVAL AVIATION SCHOOLS COMMAND (NASC); NAVAL EDUCATION AND TRAINING COMMAND (NETC); NAVAL EDUCATION TRAINING AND SECURITY ASSISTANCE FIELD ACTIVITY (NETSAFA); NAVAL HOSPITAL PENSACOLA, NAVAL LEGAL SERVICE OFFICE CENTRAL (NLSOC); REGION LEGAL SERVICE OFFICE SOUTHEAST DETACHMENT PENSACOLA; TRAWING-6; NAVAL OPERATION MEDICINE INSTITUTE (NOMI) HQ; NAVY FLIGHT DEMONSTRATION SQUADRON (BLUE ANGELS); VT-4; VT-10; VT-86; CENTER FOR INFORMATION DOMINANCE; CORRY STATION; NIOC PENSACOLA; SAUFLEY FIELD; NAVAL EDUCATION AND TRAINING PROFESSIONAL DEVELOPMENT AND TECHNOLOGY CENTER (NETPDTC); NAS WHITING FIELD MILTON FL; TRAWING-5; NAVAL SCHOOL EXPLOSIVE ORDNANCE DISPOSAL (NAVSCHOLEOD) AT EGLIN AFB

2214217 10:21 20151214 IN:SSDEMAIL #2 OUT:NCISWWSSD #2

GENERAL ADMINISTRATION 14DEC15

FROM: SEFO GEN: SE-0018

TO: DIST

SUBJ: NCIS-2 (SESL/CNSL) NCISRA ST LOUIS MO DATA SHEET

PARENT NCISFO: SOUTHEAST FIELD OFFICE MAYPORT FL (SEFO) SUBORDINATE NCISRU: SEMT/CNMT, SEDA/CNDA (FRAUD ONLY)

NOTE: NCISRA ST LOUIS MO is no longer under the ADCON/OPCON of Central Field Office as of 01NOV15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNSL, assigned to NCISRA ST LOUIS MO, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code SESL/NCISRA ST LOUIS MO will not be used until NJIS comes online. Please copy SEFO/CNMT, as appropriate. All other correspondence will utilize SESL.

MAILING ADDRESS LOCAL ADDRESS
NCISRA ST LOUIS NCISRA ST LOUIS
1 ARCHIVES DRIVE SUITE 350 1 ARCHIVES DRIVE SUITE 350
ST LOUIS, MO 63138 ST LOUIS, MO 63138

TELEPHONES COMMERCIAL NO DSN AVAILABLE
OFFICE: (314)538-2323/4
UNCLAS FAX: (314)538-2325
AFTER HOURS: b7E (DUTY CELLPHONE)

**********NO SIPRNET CAPABILITY**********

NMSG PLA: NAVCRIMINSERVRA ST LOUIS MO
NCIC/ NLETS ORI: NONE
UIC: 34418

TERRITORIAL COVERAGE:
MISSOURI: ALL COUNTIES
ILLINOIS: SOUTHERN AREA
ADDITIONALLY: RECORD INQUIRIES FOR THE NATIONAL PERSONNEL RECORDS CENTER (NPRC) AND VETERANS AFFAIRS OFFICE

PRINCIPAL INSTALLATIONS SERVICED:
NATIONAL PERSONNEL RECORDS CENTER (NPRC), ST LOUIS, MO; FORT LEONARDWOOD, MO; MCDONNELL-BOEING CORP, ST LOUIS, MO; MARCORCRUITSTA, ST LOUIS, MO; NOSC ST LOUIS, MO; NOSC SPRINGFIELD, MO; NOSC KANSAS CITY, MO; NOSC CAPE GIRARDEAU, MO; NROTCU, COLUMBIA, MO; SCOTT AIR FORCE BASE, IL

FOR OFFICIAL USE ONLY
PAGE 1 LAST (b)(6)

2214329 10:45 20151214 IN:SSDEMAIL #10 OUT:NCISWWSSD #10

GENERAL ADMINISTRATION 14DEC15

FROM: SEFO GEN: SE-0027

TO: DIST

SUBJ: NCIS-2 (SESO/CNSO) NCISRA SAN ANTONIO DATA SHEET

PARENT NCISFO: SEFO
PARENT NCISRA: SEDA/CNDA

NOTE: NCISRU SAN ANTONIO TX is no longer under the ADCON/OPCON control of Central Field Office as of 01NOV15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNSO, assigned to NCISRU SAN ANTONIO TX, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code SEC0/NCISRU SAN ANTONIO TX will not be used until NJIS comes online. Please copy SEFO/CNDA, as appropriate. All other correspondence will utilize SESO.

MAILING ADDRESS	LOCAL ADDRESS
OFFICE OF SPECIAL INVESTIGATIONS	OFFICE OF SPECIAL INVESTIGATIONS
ATTN: NCIS	ATTN: NCIS
2170 KENLY AVE	2170 KENLY AVE
LACKLAND AFB TX 78236	LACKLAND AFB TX 78236

TELEPHONES	COMMERCIAL	DSN
OFFICE	NONE	NONE
CELL PHONE	(361) 799-1157	
	(361) 533-7656	
UNCLAS FAX	(210) 671-4764 (PLEASE USE FAX COVER SHEET)	
SECURE FAX	NONE	

NMSG PLA: NAVCRIMINVSERVRA DALLAS TX
NCIS/NLET ORI NONE
UIC: 67981

TERRITORIAL COVERAGE:
MAJOR CITIES INCLUDE: SAN ANTONIO, AUSTIN, DEL RIO, EAGLE PASS, GEORGETOWN, SAN MARCOS, BRYAN, LAREDO

THE FOLLOWING COUNTIES: ATACOSA; BANDARA; BASTRUP; BEXAR; BLANCO; BREWSTER; CALDWELL; COMAL; CROCKET; DIMMIT; EDWARDS; FAYETTE; FRIO; GILLESPIE; GONZALES; GUADALUPE; HAYS; IRION; KENDALL; KERR; KIMBLE; KINNEY; LA SALLE; LAVACA; LEE; LLANO; MASON; MAVERICK;

MCCULLOCH; MEDINA; MILAM; PECOS; REAGAN; REAL; ROBERTSON; SAN SABA; SCHLEICHER; STARR; SUTTON; TRAVIS; UPTON; UVALDE; VAL VERDE; WASHINGTON; WILSON; WEBB; ZAPATA; ZAVALA

PRINCIPAL INSTALLATION SERVICED: NIOC SAN ANTONIO; NTTC DET SAN ANTONIO; NAVRESCEN SAN ANTONIO; NAVRESCEN AUSTIN; 4TH RECON BN; 4TH MARDIV; NRD SAN ANTONIO; NAVMEDTRACEN SAN ANTONIO; NOSC AUSTIN, TX;

14DEC15

SUBJ: NCIS-2 (SESO/CNSO) NCISRA SAN ANTONIO DATA SHEET

NOSC SAN ANTONIO, TX; H CO, MCSB MTEC; RANDOLPH AFB DLI; LACKLAND AFB; NSGA MEDINA SAN ANTONIO; MCRD SAN ANTONIO

1693857 16:08 20150529 IN:SSDEMAIL #8 OUT:NCISWWSSD #8

GENERAL ADMINISTRATION 28MAY15

FROM: SWND GEN: ND-0011

TO: DIST

SUBJ: **CORRECTED COPY**NCIS-2: (SWXE) NCISREP USS ESSEX (LHD 2)
DATA SHEET

ADCON: SWXE OPCON: SWXE

Mailing Address:
NCISREP USS ESSEX (LHD 2)
ATTN SAA (b)(6)
USS ESSEX (LHD 2)
FPO AP 96643-1661

NMSG PLA: NAVCRIMINVSERVREP XRAY ECHO//SWXE (PENDING)

The NCIS agent assigned to USS Essex (LHD 2) is Special Agent Afloat (b)(6) who will provide criminal, force protection, counterterrorism and counterintelligence support to all serviced commands. Send all leads to SWXE with an info copy to SWND.

Commands Serviced:
COMPHIBRON THREE (CPR-3)
USS ESSEX (LHD 2)
USS ANCHORAGE (LPD 23)
USS RUSHMORE (LSD 47)
15TH MARINE EXPEDITIONARY UNIT (15TH MEU)

(b)(6)

DISTRIBUTION
NCISHQ: ALL DEPARTMENTS AND DIRECTORATES
INFO: WWSSD

FOR OFFICIAL USE ONLY
PAGE 1 LAST (b)(6)

1971693 12:52 20150904 IN:SSDEMAIL #1 OUT:NCISWWSSD #1

GENERAL ADMINISTRATION 04SEP15

FROM: CALE GEN: LE-0014

TO: DIST

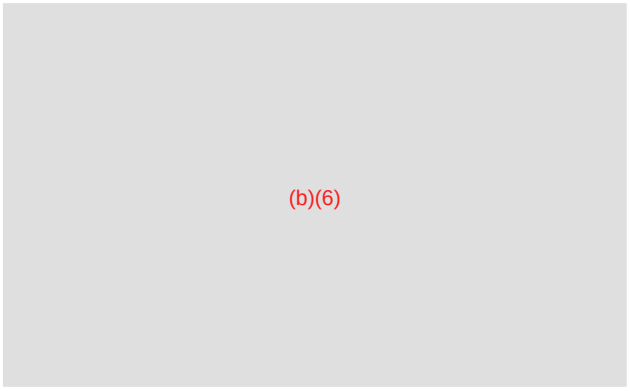
SUBJ: CAFO KEY PERSONNEL LISTING

MAILING ADDRESS:
SPECIAL AGENT IN CHARGE
NAVAL CRIMINAL INVESTIGATIVE SERVICE
Bldg. H-32 JULIAN C. SMITH DRIVE
CAMP LEJEUNE NC 28547

DMS PLA: NAVCRIMINVSERVFO CAROLINAS CAMP LEJEUNE NC

TELEPHONES: COMMERCIAL: (910) 451-8600 DSN: 751-8600 UNCLASS FAX: (910) 451-8206

(b)(6)

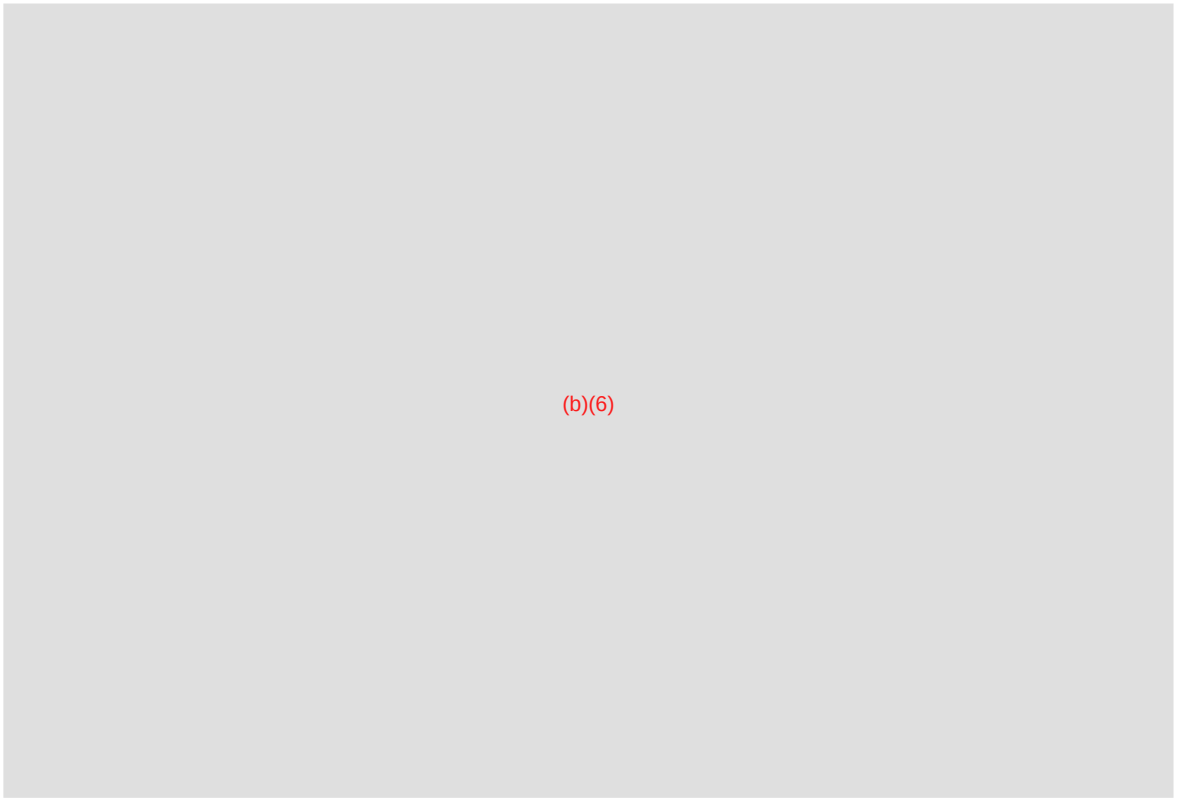


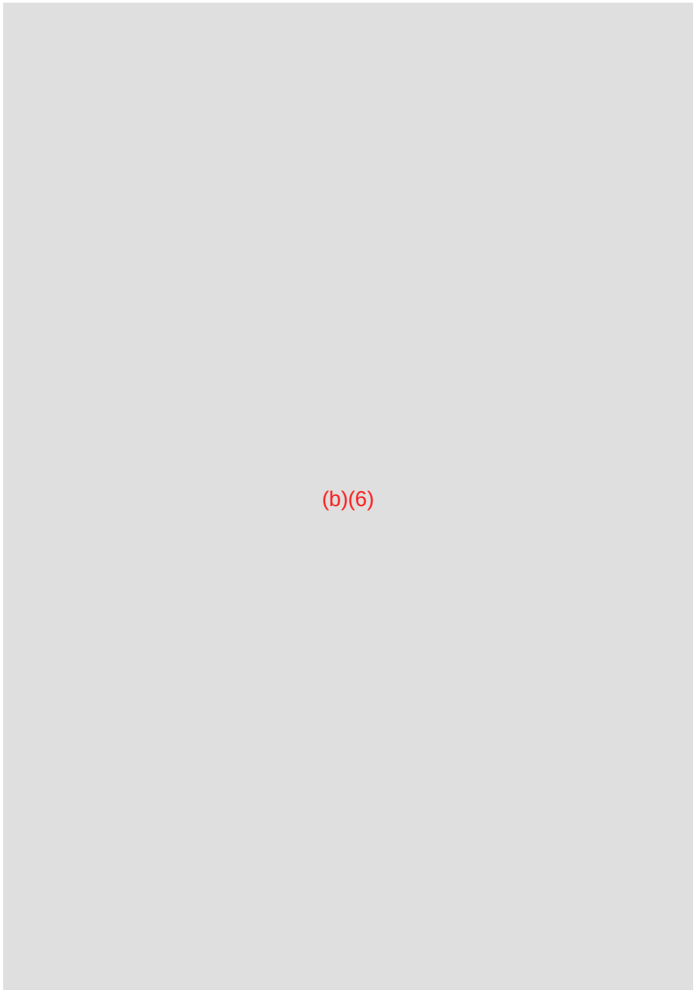
SUPERVISORY SPECIAL AGENT - FAMILY AND SEXUAL VIOLENCE (CHILD) (b)(6)

FOR OFFICIAL USE ONLY
PAGE 1

04SEP15

SUBJ: CAFO KEY PERSONNEL LISTING



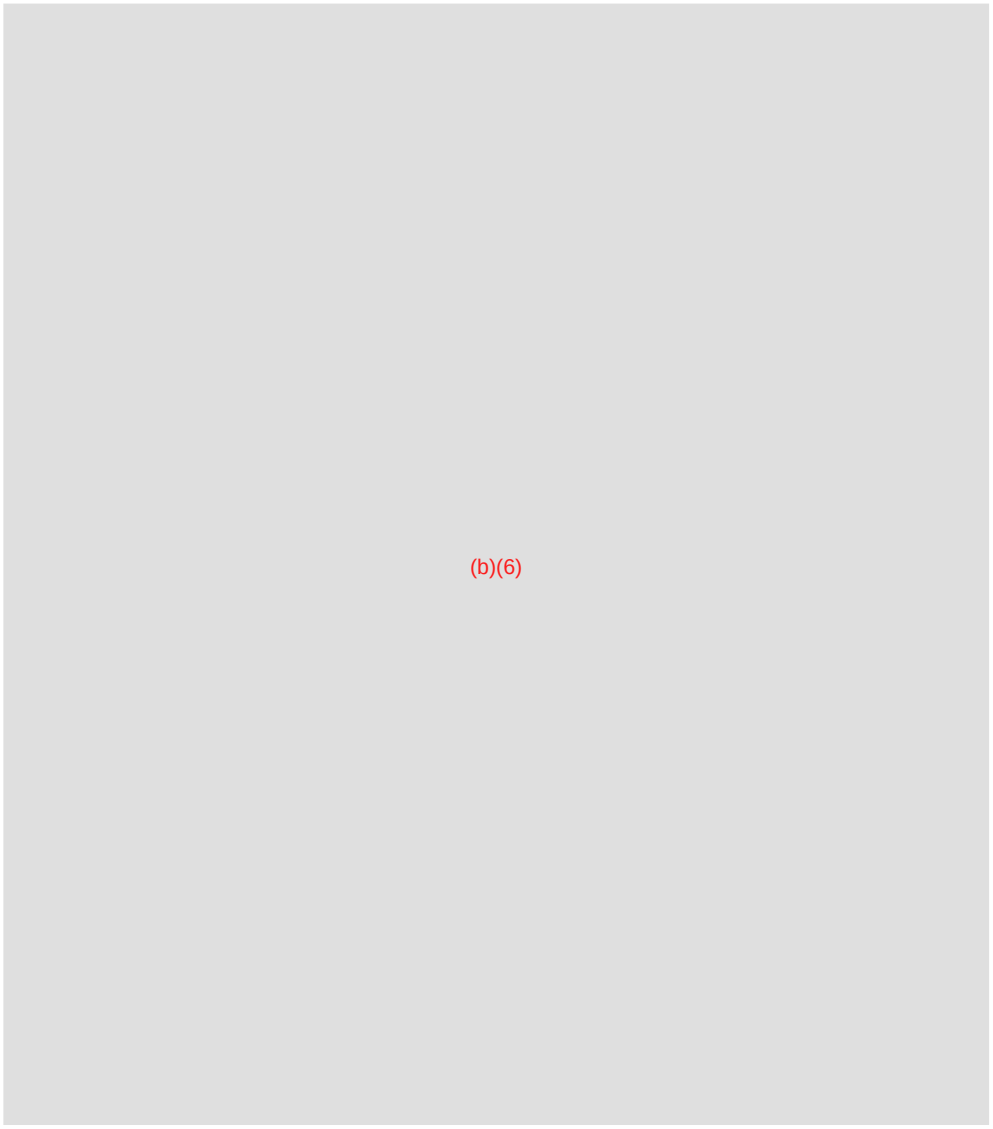


04SEP15

SUBJ: CAFO KEY PERSONNEL LISTING

FIELD COMPUTER SPECIALIST - VACANT
OFFICE: (b)(6)
MOBILE:
RESIDENCE:

INVESTIGATIVE SPECIALIST (CI/CT)



DISTRIBUTION:
INFO: ALL NCIS FO & HQ DIRECTORATE

1832795 15:38 20150717 IN:SSDEMAIL #7 OUT:NCISWWSSD #3

GENERAL ADMINISTRATION 17JUL15

FROM: CALE GEN: LE-0010

TO: DIST

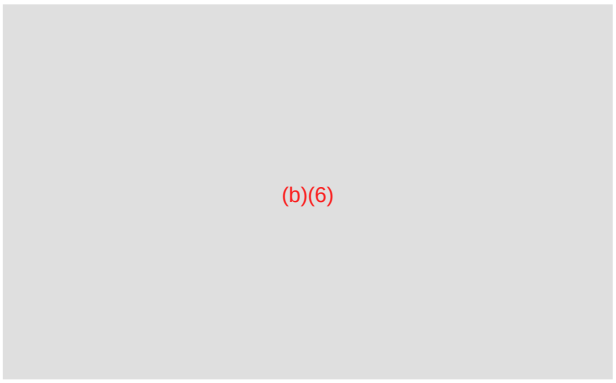
SUBJ: CAFO KEY PERSONNEL LISTING **CORRECTED COPY**

MAILING ADDRESS:
SPECIAL AGENT IN CHARGE
NAVAL CRIMINAL INVESTIGATIVE SERVICE
H 32 JULIAN C SMITH DRIVE
CAMP LEJEUNE NC 28547

DMS PLA: NAVCRIMINVSERVFO CAROLINAS CAMP LEJEUNE NC

TELEPHONES: COMMERCIAL: (910) 451-8600 DSN: 751-8600 UNCLASS FAX: (910) 451-8206

(b)(6)

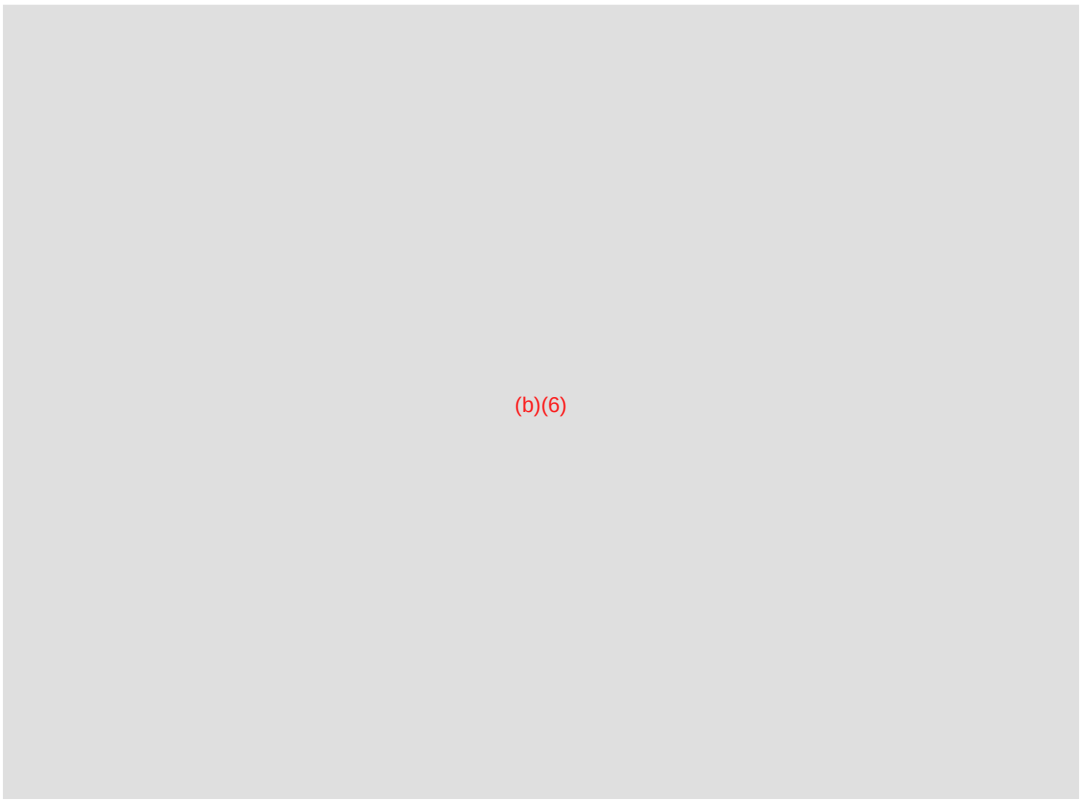


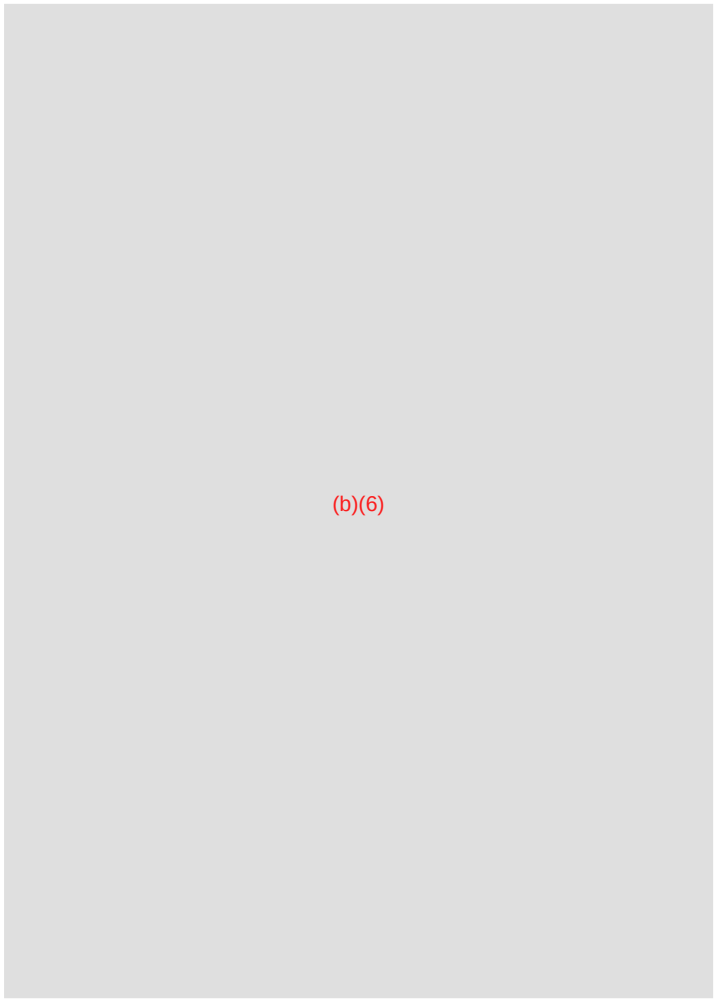
SUPERVISORY SPECIAL AGENT - FAMILY AND SEXUAL VIOLENCE (b)(6)

FOR OFFICIAL USE ONLY
PAGE 1

17JUL15

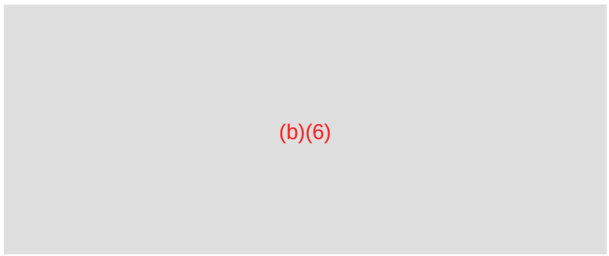
SUBJ: CAFO KEY PERSONNEL LISTING **CORRECTED COPY**

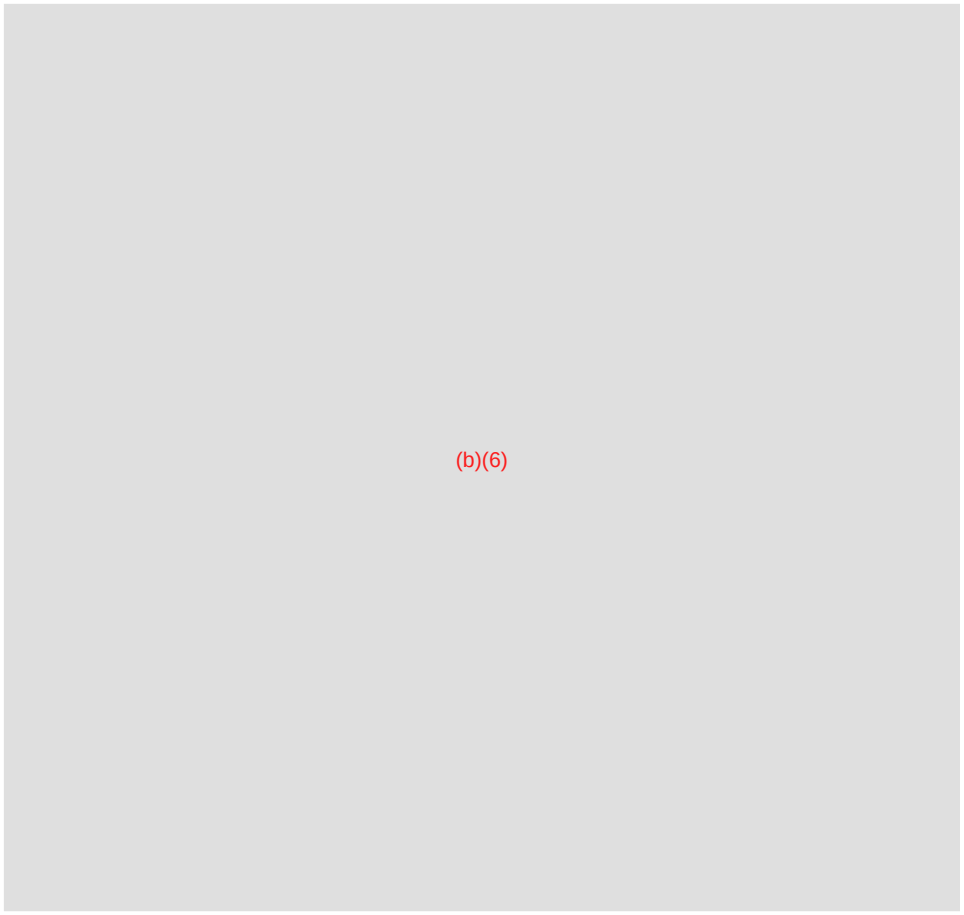




17JUL15

SUBJ: CAFO KEY PERSONNEL LISTING **CORRECTED COPY**





DISTRIBUTION
INFO: CAFO/WWSSD

2126692 14:54 20151104 IN:SSDEMAIL #4 OUT:NCISWWSSD #3

GENERAL ADMINISTRATION 04NOV15

FROM: 0000 GEN: 00-0017

TO: DIST

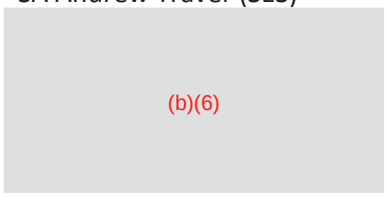
SUBJ: NCIS 2 (CODE 00) EXECUTIVE STAFF KEY PERSONNEL

MAILING ADDRESS

Naval Criminal Investigative Service
Russell-Knox Building
27130 Telegraph Road
Quantico, VA 22134
(571) 305-9000 (Front Office)
(571) 305-9115 (Facsimile)

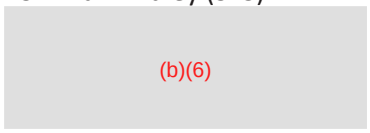
SENIOR LEADERSHIP

Director
SA Andrew Traver (SES)



Executive Assistant, Director

Deputy Director
SA Mark Ridley (SES)



(b)(6)

Executive Assistant, Deputy Director

(b)(6)

Principal Executive Assistant Director, Management & Administration SA Samuel Worth (SES)

(b)(6)

FOR OFFICIAL USE ONLY
PAGE 1

04NOV15

SUBJ: NCIS 2 (CODE 00) EXECUTIVE STAFF KEY PERSONNEL

(b)(6)

Executive Assistant, Principal Executive Assistant Director, Management & Administration SA (b)(6)

(b)(6)

Executive Assistant Director, Global Operations Directorate SA Rod Baldwin (SES)

(b)(6)

Executive Assistant, Executive Assistant Director, Global Operations Directorate SA (b)(6)

(b)(6)

Senior Intelligence Officer 02G/ Global Operations Mr. (b)(6)

(b)(6)

Executive Assistant Director, Criminal Investigations and Operations Directorate SA Andy Hogan (SES)

(b)(6)

Assistant Director, Criminal Investigations and Operations Directorate SA (b)(6)

(b)(6)

Executive Assistant Director, Intelligence and Information Sharing Directorate SA Chris Cote (DISL)

04NOV15

SUBJ: NCIS 2 (CODE 00) EXECUTIVE STAFF KEY PERSONNEL

(b)(6)

Senior Intelligence Officer, Intelligence and Information Sharing Directorate Mr. Rick Karakadze (DISL)

(b)(6)

Assistant Director, Intelligence and Information Sharing Directorate SA Mark Russ

(b)(6)

(b)(6)

Executive Assistant Director, Atlantic Operations SA Chuck May (SES)

(b)(6)

Executive Assistant, Executive Assistant Director, Atlantic Operations SA (b)(6)

(b)(6)

Acting Executive Assistant Director, Pacific Operations SA (b)(6)

(b)(6)

Executive Assistant, Executive Assistant Director, Pacific Operations Vacant

(b)(6)

Acting Executive Assistant Director, National Security Directorate SA (b)(6)

(b)(6)

04NOV15

SUBJ: NCIS 2 (CODE 00) EXECUTIVE STAFF KEY PERSONNEL

Chief, Strategic Planning

(b)(6)

(b)(6)

Principal Computer Scientist, Strategic Planning Mr. Edward So (DISL)

(b)(6)

Senior Advisor, Congressional and Media Affairs Mr. (b)(6)

(b)(6)

Senior Policy Advisor

(b)(6)

EXECUTIVE STAFF

Chief of Staff

(b)(6)

Executive Writer and Editor

(b)(6)

Inspector General

(b)(6)

Counsel

04NOV15

SUBJ: NCIS 2 (CODE 00) EXECUTIVE STAFF KEY PERSONNEL

(b)(6)

Comptroller

(b)(6)

Communications Director

(b)(6)

Ombudsman

(b)(6)

Senior Representative, SECNAV/OPNAV Staffs SA (b)(6)

(b)(6)

Assistant Director, Human Resources Directorate SA (b)(6)

(b)(6)

Security Manager

(b)(6)

Assistant Director, Command Information Officer, Information Systems Directorate Mr. (b)(6)

(b)(6)

04NOV15

SUBJ: NCIS 2 (CODE 00) EXECUTIVE STAFF KEY PERSONNEL

(b)(6)

Assistant Director - Manpower, Planning and Support Mr (b)(6)

(b)(6)

Commanding Officer, Office of Military Support CAPT (b)(6)

(b)(6)

Senior Representative, USMC HQ Staff

(b)(6)

Supervisory Executive Assistant

(b)(6)

Lead Executive Staff Assistant

(b)(6)

Executive Staff Assistant
Vacant

(b)(6)

Executive Staff Assistant (Pentagon)

(b)(6)

Distribution:
NCISHQ: ALL DEPARTMENTS AND DIRECTORATES
INFO: WWSSD/AFLT

FOR OFFICIAL USE ONLY
PAGE 6 LAST (b)(6)

2181088 09:39 20151201 IN:SSDEMAIL #5 OUT:NCISWWSSD #4

GENERAL ADMINISTRATION 01DEC15

FROM: 011C GEN: 11C-0027

TO: DISTRIBUTION

SUBJ: MANPOWER, PLANNING AND SUPPORT DIRECTORATE KEY PERSONNEL AND DATA SHEET

NCIS-2: MANPOWER, PLANNING AND SUPPORT DIRECTORATE KEY PERSONNEL AND DATA SHEET

MAILING ADDRESS
NAVAL CRIMINAL INVESTIGATIVE SERVICE HQ
ATTN: CODE 11C
27130 TELEGRAPH ROAD
QUANTICO, VA 22134

Manpower, Planning & Support (MPS)

(b)(6)

11A - SECURITY & FACILITIES

(b)(6)

(b)(6)

FOR OFFICIAL USE ONLY
PAGE 1

01DEC15

SUBJ: MANPOWER, PLANNING AND SUPPORT DIRECTORATE KEY PERSONNEL AND D

11A3

(b)(6)

11B - ACQUISITION & LOGISITICS

(b)(6)

(b)(6)

Procurement Analyst

11B1

(b)(6)

11B2
VACANT
Chief, Logistics Division

(b)(6)

(b)(6)

(b)(6)

Arms & Ammunition Branch Mgr.

(b)(6)

Supply & Services Branch Mgr.

11C - ADMINISTRATIVE SERVICES & RECORDS MANAGEMENT

(b)(6)

Office Manager

(b)(6)

01DEC15

SUBJ: MANPOWER, PLANNING AND SUPPORT DIRECTORATE KEY PERSONNEL AND D

(b)(6)

11C1 - RECORDS MANAGEMENT

(b)(6)

Branch Head, Records Management

(b)(6)

Supervisor, Liaison Section

VACANT

(b)(6)

Supervisor, Imaging Section

11C2 - CENTRAL ADMINISTRATION

(b)(6)

14A - PLANNING & EVALUATION

(b)(6)

Evaluation Lead

14P - FISCAL PLANNING & MANPOWER

(b)(6)

2185547 12:33 20151202 IN:SSDEMAIL #7 OUT:NCISWWSSD #2

GENERAL ADMINISTRATION 02DEC15

FROM: 0000 GEN: 15-0003

TO: DIST

SUBJ: NCIS-2 (CODE 15) INFORMATION TECHNOLOGY (IT) DIRECTORATE
KEY PERSONNEL DATA SHEET

MAILING ADDRESS
NAVAL CRIMINAL INVESTIGATIVE SERVICE
ATTN: CODE 15
RUSSELL-KNOX BUILDING
27130 TELEGRAPH ROAD
QUANTICO, VA 22134

UNCLAS FAX: 571-305-9994

IT SOLUTIONS CENTER: 571-305-9999
ITSC@ncis.navy.mil

Navy-ITWatch Desk
(Afterhours ITSC - Help Desk)
COML: 571-305-9438
DSN: 310-240-9438
UNCLAS FAX: COML: 571-305-9431

(b)(6)

POSITION/CODE	KEY PERSONNEL
Assistant Director/ Chief Information Officer	(b)(6)
Deputy Assistant Director Information Management	

Supervisory Program Anal
Administrative Managem

Division Chief
IT Governance (15A1)

Division Chief
Enterprise Security (15A2)

Deputy Assistant Director
Chief Technology Officer (

Division Chief
IT Project Management (1

Division Chief
Technology development

(b)(6)

Deputy Assistant Director
Enterprise Services (15C)

Division Chief
IT Operations (15C1)

Supervisory IT Specialist
IT System ADMN Branch (

Supervisory Telecommuni
IT Network/Messaging Su

Division Chief
IT Services (15C2)

Supervisory IT Specialist
Regional Computer Spec

Supervisory IT Specialist
Regional Computer Spec

Deputy Assistant Directo
IT Consolidated Support

(b)(6)

Division Chief
Information Assurance (

Division Chief
Network Operations (ITC

DISTRIBUTION
INFO: WWSSD

FOR OFFICIAL USE ONLY
PAGE 1 LAST (b)(6)

2103997 00:56 20151027 IN:SSDEMAIL #2 OUT:NCISWWSSD #1

GENERAL ADMINISTRATION 27OCT15

FROM: FEAJ GEN: AJ-0002

TO: DISTRIBUTION

SUBJ: NCIS-2 CHANGE OF ADCON/OPCON FOR USS RONALD REAGAN (CVN-76)

NOTE: NCISRA USS RONALD REAGAN HAS TRANSFERRED TO THE FAR EAST AREA OF RESPONSIBILITY. FEFO HAS ASSUMED ADCON/OPCON FOR USS RONALD REAGAN (CVN-76)

ADCON: FEFO OPCON: FEFO

PARENT NCISFO: FEFO
PARENT NCISRA: FEAJ

USS RONALD REAGAN (CVN-76) is no longer homeported in San Diego, California, and as of 01Oct15, is homeported in Yokosuka, Japan. The previous Consolidated Law Enforcement Operations Center (CLEOC) code SWXP, assigned to NCISRU RONALD REAGAN (CVN-76), is no longer accurate or valid. Due to the imminent implementation of the Navy Justice Information System (NJIS), no new CLEOC code for NCISRU RONALD REAGAN (CVN-76) will be created by NCISHQ. Therefore, for administrative purposes and oversight during the interim period, all leads intended for NCISRU RONALD REAGAN (CVN-76) should be directed to FEAJ for completion.

MAILING ADDRESS:
NCISRU RONALD REAGAN (CVN-76)
ATTN SPECIAL AGENT AFLOAT
USS RONALD REAGAN (CVN-76)
FPO AP 96616

(b)(6)

EMAIL (NCIS)
(b)(6) @ncis.navy.mil

UIC: 21412

DISTRIBUTION
WWSSD

FOR OFFICIAL USE ONLY
PAGE 1 LAST (b)(6)

1699527 08:57 20150602 IN:SSDEMAIL #1 OUT:NCISWWSSD #1

GENERAL ADMINISTRATION 02JUN15

FROM: CBFO GEN: CYB-0001

TO: DIST

SUBJ: CYBER OPERATIONS FIELD OFFICE KEY PERSONNEL (CBFO)

CYBER OPERATIONS FIELD OFFICE-(CBFO)

TITLE PERSONNEL	CONTACT NUMBERS
SAC	(b)(6)
FOS	
SIS	

ATLANTIC CYBER OPERATIONS-(CBAW)

TITLE PERSONNEL	CONTACT NUMBERS
ASA Atla	(b)(6)
SSA Wa	
SSA Wa	

SSA
Nor (b)(6)

FOR OFFICIAL USE ONLY
PAGE 1

02JUN15

SUBJ: DFLSDJFS

PACIFIC CYBER OPERATIONS - (CBPW)
TITLE PERSONNEL CONTACT NUMBERS

ASA
Paci

SSA (b)(6)

FOR OFFICIAL USE ONLY
PAGE 1

29APR14

SUBJ: CYBER OPERATIONS FIELD OFFICE KEY PERSONNEL (CBFO)

SSA (b)(6)

SSA (b)(6)

DISTRIBUTION
NCISHQ: ALL Departments and Directorates
INFO: WWSSD/AFLT

FOR OFFICIAL USE ONLY
PAGE 2 LAST (b)(6)

1906532 18:37 20150812 IN:SSDEMAIL #5 OUT:NCISWWSSD #1

GENERAL ADMINISTRATION 12AUG15

FROM: 002P GEN: O2P-0001

TO: DIST

SUBJ: EXECUTIVE ASSISTANT DIRECTOR FOR PACIFIC OPERATIONS KEY PERSONNEL LISTING

MAILING ADDRESS:
NCIS EADPAC
NAVBASE POINT LOMA
140 SYLVESTER ROAD, BLDG. 138
SAN DIEGO, CA 92106-3251

DMS PLA: NAVCRIMINVSERV EADPAC SAN DIEGO CA

TELEPHONES: COMMERCIAL: (CONUS 011) DSN: (312) UNCLAS PHONE: 619 553 6835
UNCLAS FAX: 619 553-7048

EADPAC
OFFICE:
COMM
CELL: (b)(6)

CHIEF STAFF OFFICER (b)(6)
OFFICE:
COMME (b)(6)
CELL:

EXECUTIVE ASSISTANT (b)(6)
OFFICE:
COMME (b)(6)
CELL:

EXECUTIVE SECRETARY (b)(6)
OFFICE:
COMMER (b)(6)
CELL: TBD

PSYCHOLOGIST DR. (b)(6)
OFFICE:
COMME (b)(6)
CELL:

DESK OFFICER (VACANT)
OFFICE:
COMMER (b)(6)
CELL: TBD

DESK OFFICER (VACANT) - (incoming (b)(6)
OFFICE: (b)(6)

FOR OFFICIAL USE ONLY
PAGE 1

12AUG15

SUBJ: EXECUTIVE ASSISTANT DIRECTOR FOR PACIFIC OPERATIONS KEY PERSON

COMMERCIAL: (b)(6)
CELL: TBD

DESK OFFICER SA (b)(6)
OFFICE:
COMME (b)(6)
CELL:

STAFF JUDGE ADVOCATE LT (b)(6)
OFFICE:
COMME (b)(6)
CELL:

SENIOR INTEL OFFICER (b)(6)
OFFICE:
COMMER (b)(6)
CELL: TBD

C-CICA
OFFICE (b)(6)

COMME (b)(6)
CELL:

FOR OFFICIAL USE ONLY
PAGE 2 LAST (b)(6)

GENERAL ADMINISTRATION 18FEB16

FROM: FESS GEN: SS-0001

TO: DIST

SUBJ: NCIS-2 (FEX6) NCISRU USS BONHOMME RICHARD (LHD-6) DATA SHEET

ADCON: FEFO
OPCON: FEFO

PARENT NCISFO: FEFO
PARENT NCISRA: FESS

NOTE: LEADS SHOULD BE DIRECTED TO FEX6 WITH AN INFORMATION COPY TO NCISRA SASEBO, JAPAN (FESS). PRIOR TO SENDING LEADS TO FEX6, CONTACT FESS VIA DSN PHONE AT 315-252-3621.

MAILING ADDRESS:
SPECIAL AGENT AFLOAT
USS BONHOMME RICHARD (LHD-6)
NAVAL CRIMINAL INVESTIGATIVE SERVICE
UNIT 100184 BOX 617
FPO AP 96617

TELEPHONE DSN
OFFICE 315-453-7245

UIC: 34451

DISTRIBUTION
INFO: WWSSD

FOR OFFICIAL USE ONLY
PAGE 1 LAST (b)(6)

1501974 16:32 20150316 IN:SSDEMAIL #3 OUT:NCISWWSSD #1

GENERAL ADMINISTRATION 16MAR15

FROM: HIFO GEN: HN-0003

TO: DIST

SUBJ: NCIS-2/(HIFO) NCISFO HAWAII KEY PERSONNEL LISTING

CODE/POSITION KEY PERSONNEL

SAC

ASAC
(CRIM)

(NSD)

(b)(6)

SIO

FOSO

SSA (CRIM

SSA (HIKH)

(b)(6)

FOR OFFICIAL USE ONLY
PAGE 1

16MAR15

SUBJ: NCIS-2/(HIFO) NCISFO HAWAII KEY PERSONNEL LISTING

SSA (HIMI)

SPA

EVID
CUSTODIA

FCS

(b)(6)

PACOM

(b)(6)

PACFLT

CI SUPPORT ELEMENT TO PACOM
SA

JTTF
SA

(b)(6)

2GJV

FOR OFFICIAL USE ONLY
PAGE 2

16MAR15

SUBJ: NCIS-2/(HIFO) NCISFO HAWAII KEY PERSONNEL LISTING

(b)(6)

2GTH
SA

(b)(6)

FORENSIC CONSULTANT (b)(6)
SA

(b)(6)

INFO: WWSSD

1753292 07:47 20150618 IN:SSDEMAIL #2 OUT:NCISWWSSD #1

GENERAL ADMINISTRATION 18JUN15

FROM: MEBJ GEN: BJ-0015

TO: DIST

SUBJ: NICS-2: (MEFO) NCIS MIDDLE EAST FIELD OFFICE KEY PERSONNEL

CODE: MEBJ
COMM FROM THE U.S.: 011 + COUNTRY CODE + TEL # MOBILE FROM THE U.S.: 011 + COUNTRY CODE + CELL# WITHIN THE MIDDLE EAST OR FROM EUROPE: 00 + COUNTRY CODE + TEL # DSN PREFIX FOR BAHRAIN: 318

POSITION KEY PERSONNEL

(b)(6)

(b)(6)

SSA FP/TMU VACANT (SOLOMON HAGEDON INBOUND 7/15)

(b)(6)

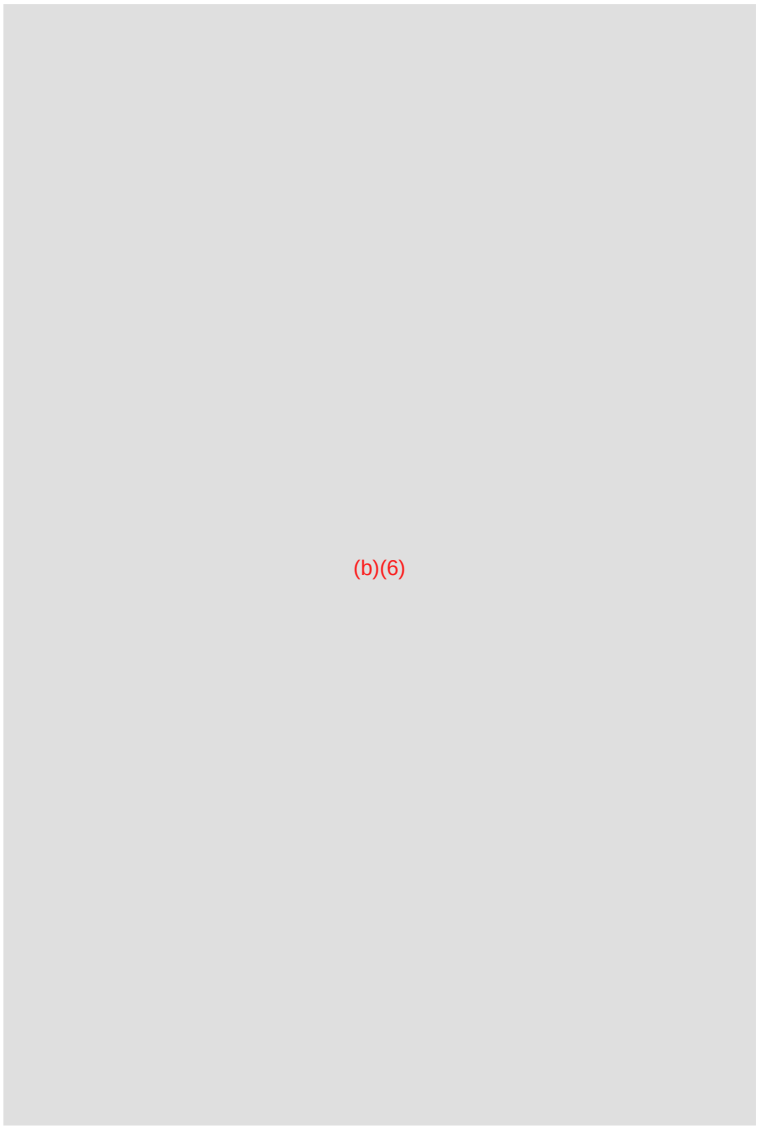
FOR OFFICIAL USE ONLY
PAGE 1

18JUN15

SUBJ: NICS-2: (MEFO) NCIS MIDDLE EAST FIELD OFFICE KEY PERSONNEL

(b)(6)

(b)(6)



18JUN15

SUBJ: NICS-2: (MEFO) NCIS MIDDLE EAST FIELD OFFICE KEY PERSONNEL

(b)(6)

(b)(6)

DISTRIBUTION
NCISHQ: ALL DIRECTORATES AND DEPARTMENTS
INFO: WWSSD/MEBJ

2363892 02:07 20160207 IN:SSDEMAIL #1 OUT:NCISWWSSD #1

GENERAL ADMINISTRATION 07FEB16

FROM: MEBJ GEN: BJ-0003

TO: DIST

SUBJ: NCIS-2: (MEKP) NCIS MIDDLE EAST FIELD OFFICE KEY PERSONNEL

CODE: MEBJ

DIALING INSTRUCTIONS:
FROM THE US: 011 + COUNTRY CODE + TEL#
WITHIN THE MIDDLE EAST/EUROPE: 00 + COUNTRY CODE + NUMBER DSN PREFIX FOR BAHRAIN: 318

MIDDLE EAST FIELD OFFICE KEY PERSONNEL

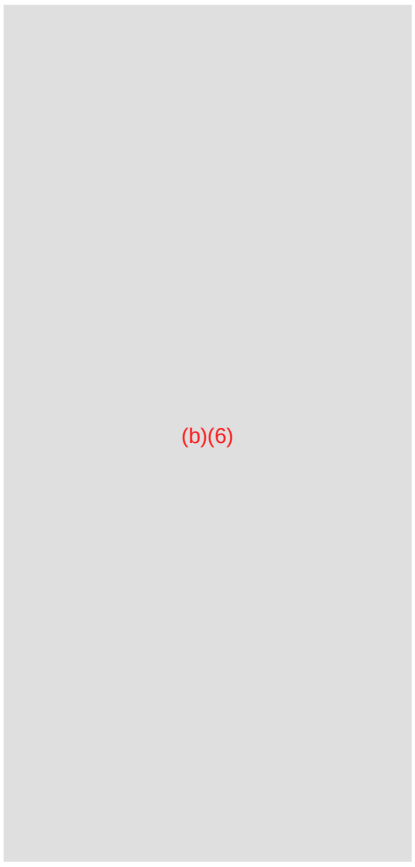
(b)(6)

CHIEF TRANSNATIONAL CRIMES UNIT (TCU) (b)(6)

(b)(6)

07FEB16

SUBJ: NCIS-2: (MEKP) NCIS MIDDLE EAST FIELD OFFICE KEY PERSONNEL



MEDB - NCISRA DUBAI, UAE

(b)(6)

MEDJ - NCISRA DJIBOUTI

(b)(6)

MEDJ

(b)(6)

MEEG - FPD EGYPT

(b)(6)

MEUM - FPD MAURITIUS

(b)(6)

07FEB16

SUBJ: NCIS-2: (MEKP) NCIS MIDDLE EAST FIELD OFFICE KEY PERSONNEL

MEKE - FPD KENYA

(b)(6)

FPD JORDAN

(b)(6)

DISTRIBUTION
INFO: WWSSD

FOR OFFICIAL USE ONLY

2262017 15:47 20160105 IN:SSDEMAIL #20 OUT:NCISWWSSD #15

GENERAL ADMINISTRATION 05JAN16

FROM: NENP GEN: NP-0002

TO: DIST

SUBJ: NCIS-2/(NEBN BOSTON-JTTF) NCIS REPRESENTATIVE TO THE FBI
JOINT TERRORIST TASK FORCE (JTTF) DATA SHEET

NOTE: ANY NCIS CAT 5 INVESTIGATIVE LEADS TO THE NEBN BOSTON-JTTF REP SHOULD ALSO INCLUDE THE FCI SSA AT NENP AND THE FCI ASAC AT NENP ON DISTRIBUTION FOR CASE TRACKING AND ADMINISTRATIVE PURPOSES.

PARENT NCISFO: NORTHEAST FIELD OFFICE, NEWPORT, RI PARENT NCISRA: NEWPORT, RI (NENP)

MAILING & LOCAL ADDRESS
NCIS REPRESENTATIVE
FBI
ONE CENTER PLAZA
SQUAD CT-1
BOSTON, MA 02108

TELEPHONES	COMMERICAL
DIRECT LINE (NCIS REP)	(617) 223-6452
GENERAL NUMBER	(617) 742-5533
AGENTS CELL	(617) 680-7242

UNCLAS FACSIMILE (NCIS REP) (617) 223-6545

NMSG PLA: NONE
USE: NAVCRIMINVSERVFO NORTHEAST NEWPORT RI NCIC/NLETS ORI: NONE
UIC: 67985

AFTER HOURS (617) 742-5533
(FBI BOS DUTY AGENT AND OPERATIONS CENTER)

THE FBI/BOSTON OPERATIONS CENTER DUTY AGENT CAN REACH THE NCIS REPRESENTATIVE TO THE JTTF, SQUAD CT-1.

COVERAGE:
THE FBI JTTF HAS JURISDICTIONAL RESPONSIBILITY FOR CONDUCTING BOTH DOMESTIC AND INTERNATIONAL COUNTERTERRORISM INVESTIGATIONS WITHIN THE CONFINES OF THE CITY OF BOSTON AND SURROUNDING COUNTIES (SUFFOLK COUNTY, SOUTHERN ESSEX AND MIDDLESEX COUNTIES, NORTHERN NORFOLK AND PLYMOUTH COUNTIES)

DISTRIBUTION
INFO: WWSSD

FOR OFFICIAL USE ONLY
PAGE 1 LAST (b)(6)

2261210 13:11 20160105 IN:SSDEMAIL #9 OUT:NCISWWSSD #8

GENERAL ADMINISTRATION 28DEC15

FROM: NENP GEN: NP-0010

TO: DIST

SUBJ: NCIS-2: (NECA/CNCL) NCISRU CRANE DATA SHEET

PARENT NCISFO: NORTHEAST FIELD OFFICE, NEWPORT, RI (NENP) PARENT NCISRA: GREAT LAKES, IL (NEGL)

NOTE: NCISRU CRANE IN is no longer under the ADCON/OPCON of Central Field Office as of 01NOV15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNCA, assigned to NCISRA CRANE IL, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code NECA/NCISRU CRANE IN will not be used until NJIS comes online. Please copy NENP, as appropriate. All other correspondence will utilize NECA

MAILING ADDRESS/LOCAL ADDRESS
NCISRU CRANE
NSWC 300 HWY 361
BLDG 121 RM 214
CRANE IN 47522-5000

TELEPHONES COMMERCIAL DSN
OFFICE: (812)854-4402 482-4402
UNCLAS FAX: (812)854-3461 482-3461
STU-III: (812)854-1257 482-1257
AFTER HOURS: (812)854-3300 482-3300

NMSG PLA: NAVCRIMINVSERVREP CRANE IN
NLET/NCIC ORI: NONE
UIC: NONE - USE NEGL: 42919

TERRITORIAL COVERAGE:
FCI COVERAGE AS DIRECTED BY NCISFO NORTHEAST

PRINCIPAL INSTALLATIONS SERVICED:
NSWC CRANE DIVISION, CRANE, IN
NSWC DET LOUISVILLE, KY

DISTRIBUTION
WWSSD

FOR OFFICIAL USE ONLY
PAGE 1 LAST (b)(6)

2261217 13:13 20160105 IN:SSDEMAIL #11 OUT:NCISWWSSD #10

GENERAL ADMINISTRATION 28DEC15

FROM: NENP GEN: NP-0009

TO: DIST

SUBJ: NCIS-2: (NECL/CNCL) NCISRU CLEVELAND DATA SHEET

PARENT NCISFO: NORTHEAST FIELD OFFICE, NEWPORT, RI (NENP) PARENT NCISRA: GREAT LAKES, IL (NEGL)

NOTE: NCISRU CLEVELAND OH is no longer under the ADCON/OPCON of Central Field Office as of 01OCT15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNCL, assigned to NCISRA CLEVELAND OH, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code NECL/NCISRU CLEVELAND OH will not be used until NJIS comes online. Please copy NEFO, as appropriate. All other correspondence will utilize NECL

MAILING ADDRESS LOCAL ADDRESS
P. O. BOX 99809 1240 E. 9TH ST, RM 1457
CLEVELAND, OH 44199-2055 CLEVELAND, OHIO 44199-2055

TELEPHONES COMMERCIAL DSN
OFFICE: (216) 522-6774/5/6758 580-6774/5/6758 UNCLAS FACSIMILE: (216) 522-6629
STU-III: (216) 522-6774
AFTERHOURS: (216) 522-5666/23
DFAS CLEVELAND COMMUNICATIONS CENTER

NMSG PLA: none
use - NAVCRIMINVSERVFO NORTHEAST NEWPORT RI NCIC/NLETS ORI: none
UIC: NONE; USE NEGL - 42919

TERRITORIAL COVERAGE
OHIO: NON HAZARDOUS INTERVIEWS ONLY
NOTE: NCISRU CLEVELAND OH CONSISTS OF ONE (1) GS-1810 INVESTIGATOR.

PRINCIPAL INSTALLATION SERVICED
DFAS CLEVELAND OH
DFAS COLUMBUS OH

BUPERS PCS COMPONENT

DISTRIBUTION
WWSSD

FOR OFFICIAL USE ONLY
PAGE 1 LAST (b)(6)

2261711 14:23 20160105 IN:SSDEMAIL #18 OUT:NCISWWSSD #14

GENERAL ADMINISTRATION 28DEC15

FROM: NENP GEN: NP-0012

TO: DIST

SUBJ: NCIS-2: "CORRECTED COPY" (NEDY/CNDY) NCISRU DAYTON DATA SHEET

********** CI COVERAGE ONLY **********

PARENT NCISFO: NORTHEAST FIELD OFFICE, NEWPORT, RI (NENP) PARENT NCISRA: GREAT LAKES, IL (NEGL)

NOTE: NCISRU DAYTON OH is no longer under the ADCON/OPCON control of Central Field Office as of 01OCT15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNDY, assigned to NCISRU DAYTON OH, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code NEDY/NCISRU DAYTON OH will not be used until NJIS comes online. Please copy NEFO, as appropriate. All other correspondence will utilize NEDY.

MAILING ADDRESS LOCAL ADDRESS
NCIS REPRESENTATIVE NCISRU DAYTON
AFOSI REGION 1/XOQ 4375 CHIDLAW RD, BLDG 216, RM A036
4375 CHIDLAW ROAD, DOOR S007 WRIGHT PATTERSON AFB, OH 45433-5006
WRIGHT PATTERSON AFB, OH 45433-5006

TELEPHONES COMMERCIAL DSN

OFFICE STE: 937-522-2187 672-2187
CELL PHONE: 202-372-7837
FACSIMILE: 937-522-2197 (PLEASE USE FAX COVER SHEET)
SECURE FAX: (b)(6)
SSD TELECOMMUNICATIONS: NIPRNET
NMSG PLA: NAVCRIMINVSERVRA DAYTON OH
NCIS/NLET ORI NONE
UIC: 34402

TERRITORIAL COVERAGE:
EASTERN KENTUCKY AND OHIO

PRINCIPAL INSTALLATION SERVICED:
WRIGHT PATTERSON AFB, OH

DISTRIBUTION
WWSSD

FOR OFFICIAL USE ONLY
PAGE 1 LAST (b)(6)

2261154 13:07 20160105 IN:SSDEMAIL #8 OUT:NCISWWSSD #7

GENERAL ADMINISTRATION 28DEC15

FROM: NENP GEN: NP-0013

TO: DIST

SUBJ: NCIS-2: (NEGL/CNGL) NCISRA GREAT LAKES DATA SHEET

PARENT NCISFO: NORTHEAST FIELD OFFICE, NEWPORT, RI (NENP)

NOTE: NCISRA GREAT LAKES IL is no longer under the ADCON/OPCON control of Central Field Office as of 01NOV15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNGL, assigned to NCISRA GREAT LAKES IL, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code NEGL/NCISRA GREAT LAKES IL will not be used until NJIS comes online. Please copy NENP, as appropriate. All other correspondence will utilize NEGL.

MAILING ADDRESS	LOCAL ADDRESS
2540A PAUL JONES ST	2540A PAUL JONES ST
GREAT LAKES, IL 60088	GREAT LAKES, IL 60088

TELEPHONES	COMMERCIAL	DSN
OFFICE:	(847) 688-5655/6/7/5668/9	792-655/6/7/5668/9
AFTER HOURS:	(847) 688-5555	
GREAT LAKES PD: 792-5555		
PATCH NUMBER:	(847) 688-0147 CONNECT: *DISCONNECT: #	
UNCLAS FACSIMILE:	(847) 688-2636	792-2636
STE:	(847) 688-2612	792-2612

NMSG PLA: NAVCRIMINVSERVRA GREAT LAKES IL//CNGL// NCIC/NLETS ORI: NONE BASE STATION IDENTIFIER CODE (NFC): 320
UIC: 42919

TERRITORIAL COVERAGE:
INDIANA, ILLINOIS, MICHIGAN, WISCONSIN, OHIO, KENTUCKY

PRINCIPAL INSTALLATIONS SERVICED:
AIR FORCE OFFICE OF SPECIAL INVESTIGATIONS TENTH FIELD INVESTIGATIONS SQUADRON, INDIANAPOLIS, IN BUREAU OF NAVAL PERSONNEL PERMANENT CHANGE OF STATION COMPONENT,

CLEVELAND, OH DEFENSE CONTRACT MANAGEMENT AGENCY (DCMA) OFFICES IN WISCONSIN, ILLINOIS, INDIANA AND MICHIGAN DEFENSE FINANCE AND ACCOUNTING SERVICE, CLEVELAND, OH DEFENSE FINANCE AND ACCOUNTING SERVICE, COLUMBUS, OH DEFENSE FINANCE AND ACCOUNTING SERVICE INDIANAPOLIS, IN DEFENSE INFORMATION SYSTEMS AGENCY, SCOTT AFB IL DEFENSE REUTILIZATION & MARKETING REGION BATTLECREEK, MI DOD-IG DEFENSE CRIMINAL INVESTIGATIVE SERVICE (DCIS) RESIDENT AGENCY,

28DEC15

SUBJ: NCIS-2: (NEGL/CNGL) NCISRA GREAT LAKES DATA SHEET

INDIANAPOLIS, IN
MARINE OFFICER SELECTION OFFICE COLUMBUS, OH MILITARY ENTRANCE PROCESSING COMMAND, GREAT LAKES, IL NAVY AND MARINE CORPS RESERVE CENTER COLUMBUS, OH NAVAL DENTAL CLINIC GREAT LAKES, IL NAVAL STATION, GREAT LAKES, IL NAVAL SURFACE WARFARE CENTER CRANE DIVISION, CRANE, IN NAVAL SURFACE WARFARE CENTER DET LOUISVILLE, KY NAVY DENTAL RESEARCH INSTITUTE GREAT LAKES, IL NAVY EXCHANGE, GREAT LAKES, IL NAVY LEGAL SERVICE OFFICE, GREAT LAKES, IL NAVY OPERATIONAL SUPPORT CENTER, DECATUR, IL NAVY OPERATIONAL SUPPORT CENTER, PEORIA, IL NAVY OPERATIONAL SUPPORT CENTER, ROCK ISLAND, IL NAVY OPERATIONAL SUPPORT CENTER, INDIANAPOLIS, IN NAVY OPERATIONAL SUPPORT CENTER, LOUISVILLE, KY NAVY OPERATIONAL SUPPORT CENTER, BATTLE CREEK, MI NAVY OPERATIONAL SUPPORT CENTER, DETROIT, MI NAVY OPERATIONAL SUPPORT CENTER, SAGINAW, MI NAVY OPERATIONAL SUPPORT CENTER, AKRON, OH NAVY OPERATIONAL SUPPORT CENTER, CINCINNATI, OH NAVY OPERATIONAL SUPPORT CENTER, COLUMBUS, OH NAVY OPERATIONAL SUPPORT CENTER, TOLEDO, OH NAVY OPERATIONAL SUPPORT CENTER, YOUNGSTOWN, OH NAVY OPERATIONAL SUPPORT CENTER, GREEN BAY, WI NAVY OPERATIONAL SUPPORT CENTER, MADISON, WI NAVY OPERATIONAL SUPPORT CENTER, MILWAUKEE, WI NAVY REGION MID-ATLANTIC RESERVE COMPONENT COMMAND, GREAT LAKES, IL NAVY RECRUIT TRAINING COMMAND, GREAT LAKES, IL NAVY RECRUITING DISTRICT COLUMBUS, OH NAVY RECRUITING DISTRICT DETROIT, MI NAVY RECRUITING AREA FIVE, GREAT LAKES, IL NAVY RECRUITING DISTICT INDIANAPOLIS IN NAVY RECRUITING DISTRICT, MILWAUKEE, WI NAVY TRAINING CENTER, GREAT LAKES, IL PERSONNEL SUPPORT DETACHMENT, COLUMBUS, OH PERSONNEL SUPPORT DETACHMENT, GREAT LAKES, IL SERVICE SCHOOL COMMAND, GREAT LAKES, IL TRANSIENT PERSONNEL UNIT, GREAT LAKES, IL WRIGHT PATTERSON AIR FORCE BASE, OH

DISTRIBUTION
WWSSD

2261596 14:06 20160105 IN:SSDEMAIL #14 OUT:NCISWWSSD #13

GENERAL ADMINISTRATION 28DEC15

FROM: NENP GEN: NP-0011

TO: DIST

SUBJ: NCIS-2: "CORRECTED COPY" (NEIN/CNIN) NCISRU INDIANAPOLIS
DATA SHEET

PARENT NCISFO: NORTHEAST FIELD OFFICE, NEWPORT, RI (NENP) PARENT NCISRA: GREAT LAKES, IL (NEGL)

NOTE: NCISRU INDIANAPOLIS IN is no longer under the ADCON/OPCON of Central Field Office as of 01NOV15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNIN, assigned to NCISRU INDIANAPOLIS IN, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code NEIN/NCISRU INDIANAPOLIS IN will not be used until NJIS comes online. Please copy NENP, as appropriate. All other correspondence will utilize NEIN.

MAILING/LOCAL ADDRESS
NCISRU INDIANAPOLIS (FRAUD)
AFOSI 10TH FIS OPERATING L-A
111 MONUMENT CIRCLE SUITE 412
INDIANAPOLIS, IN 46204

TELEPHONES COMMERCIAL
OFFICE: (317) 226-5380
AFTER HOURS: (847) 456-4576
UNCLAS FACSIMILE: (317) 226-5134

NMSG PLA: NONE
USE - NAVCRIMINVSERVFO NORTHEAST NEWPORT RI
UIC: 34409

TERRITORIAL COVERAGE:
ONLY MAJOR PROCUREMENT FRAUD INVESTIGATIONS/LEAD COVERAGE IN THE STATES OF INDIANA, OHIO, AND MICHIGAN.

PRINCIPAL INSTALLATIONS SERVICED:

AIR FORCE OSI TENTH FIELD INVESTIGATIONS SQUADRON, INDIANAPOLIS DETACHMENT; DEFENSE FINANCE AND ACCOUNTING SERVICE INDIANAPOLIS, IN; DOD-IG DEFENSE CRIMINAL INVESTIGATIVE SERVICE (DCIS) RESIDENT AGENCY, INDIANAPOLIS, IN; DEFENSE CONTRACT MANAGEMENT AGENCY (DCMA) OFFICES IN WISCONSIN, ILLINOIS, INDIANA AND MICHIGAN.

DISTRIBUTION
WWSSD

FOR OFFICIAL USE ONLY
PAGE 1 LAST (b)(6)

GENERAL ADMINISTRATION 03FEB16

FROM: NFNF GEN: NF-0002

TO: DIST

SUBJ: NCIS - 2 (NFNF) NCISRA NORFOLK VA DATA SHEET

PARENT NCISFO: NFFO

NOTE SUBORDINATE OFFICES: NFCE, NFFM, NFHV, NFLC, NFPV, NFYT, NFXA, NFXH, NFXL, NFXO, NFXQ, NFX1, NFX3

NOTE: NCIS OFFICES UNDER NCISRA NORFOLK ARE SERVICED BY THE NCIS CENTRAL EVIDENCE FACILITY (CEF) AND EVIDENCE SHOULD BE MAILED DIRECTLY TO THEM AT: 9079 HAMPTON BLVD, SUITE 110, NORFOLK VA 23505-1098. THE LONG TERM STORAGE (LTS) FACILITY IS STILL PENDING THE TESTING AND IMPLEMENTATION OF AN ELECTRONIC CUSTODY SYSTEM. FURTHER GUIDANCE IS PENDING.

MAILING ADDRESS	LOCAL ADDRESS
NCIS NORFOLK FIELD OFFICE	BLDG U-40
1329 BELLINGER BLVD	NAVAL STATION
NORFOLK VA 23511-2310	NORFOLK VA

TELEPHONES:

OFFICE: (757) 444-7327 DSN: 564
(757) 444-1672 DSN: 564

UNCLAS FAX: (757) 444-3139 DSN: 564

AFTER HOURS:
DUTY TEXT NOTIFICATION: (757) 475-2481

NAVAL BASE:
POLICE WATCH CAPTAIN: (757) 322-2551

NCIS/NLETS ORI: VANIS0900
NMSG PLA: NAVCRIMINSVERFO NORFOLK VA//NFNF//
UIC: 45086

TERRITORIAL COVERAGE: ALL MILITARY INSTALLATIONS (SHORE AND AFLOATS) IN VIRGINIA, LESS THE COUNTIES OF: ARLINGTON, CAROLINE, CLARKE, CULPEPPER, ESSEX, FAIRFAX, FAUQUIER, FREDERICK, GREENE, KING GEORGE, LANCASTER, LOUDOUN, MADISON, NORTHCUMBERLAND, ORANGE, PAGE, PRINCE WILLIAM, RAPPAHANNOCK, RICHMOND COUNTY, ROCKINGHAM, SHENANDOAH, SPOTSYVANIA, STAFFORD, WARREN AND WESTMORELAND.

2356072 12:22 20160204 IN:SSDEMAIL #6 OUT:NCISWWSSD #4

GENERAL ADMINISTRATION 04FEB16

FROM: NFNF GEN: NF-0005

TO: DIST

SUBJ: NCIS - 2 (NFXO) NCISRU USS GEORGE WASHINGTON (CVN-73) DATA SHEET

ADCON: NFNF OPCON: NFNF

MAILING ADDRESS

ATTN: SAA - USS GEORGE WASHINGTON (CVN-73) NAVAL CRIMINAL INVESTIGATIVE SERVICE NORFOLK FIELD OFFICE
1329 BELLINGER BLVD
NORFOLK VA 23511-2310

NMSG PLA: NAVCRIMINVSERVREP XRAY OSCAR

UIC: 21412

2216105 17:14 20151214 IN:SSDEMAIL #19 OUT:NCISWWSSD #19

GENERAL ADMINISTRATION 14DEC15

FROM: NFNF GEN: NF-0044

TO: DIST

SUBJ: NCIS - 2 (NFYT) - NCISRU YORKTOWN DATA SHEET

PARENT NCISFO: NFFO
PARENT NCISRA: NFNF

NOTE: Until the Code of NFYT has been established in the Consolidated Law Enforcement Operations Center (CLEOC) around the end of January 2016, NCIS offices will use the office code of NFNF for sending leads to NCISRU Yorktown when using CLEOC.

LOCAL/MAILING ADDRESS

NCISRU YORKTOWN
2029 LONGFELLOW ROAD
NAVAL WEAPONS STATION
YORKTOWN, VA 23691-1900

TELEPHONE
OFFICE: COM - (757) 887-7305

UIC: 45188

TERRITORIAL COVERAGE: COUNTIES OF HANOVER, NEW KENT, YORK, HENRICO, CHESTERFIELD, JAMES CITY, GLOUCESTER, GOOCHLAND, POWHATAN, MIDDLESEX, MATTHEWS AND POQUOSON AND THE NEARBY CITIES OF RICHMOND, WILLIAMSBURG, HAMPTON AND NEWPORT NEWS.

2235609 08:35 20151222 IN:SSDEMAIL #1 OUT:NCISWWSSD #1

GENERAL ADMINISTRATION 22DEC15

FROM: 0022 GEN: 22-0015

TO: DIST

SUBJ: NCIS-2/NATIONAL SECURITY DIRECTORATE KEY PERSONNEL DATA SHEET (0022)

MAILING ADDRESS
NAVAL CRIMINAL INVESTIGATIVE SERVICE
HEADQUARTERS (NCISHQ CODE 0022)
27130 TELEGRAPH ROAD
QUANTICO, VA 22134

TELEPHONES
DSN PREFIX: INCOMING 240-XXXX (LAST 4)
OUTGOING 94-XXX-XXXX (CONUS)
OUTGOING 94-312-XXX-XXXX (OCONUS)
OFFICE: 571-305-9689 (TEMP)
UNCLASS FAX: 571-305-9574
SECURE FAX: (b)(6)

NAVMSG PLA: NAVCRIMINVSERVHQ NSD QUANTICO VA

CODE/PERSONNEL TELEPHONE NUMBERS

EXECUTIVE ASSISTANT DIRECTOR OFFICE: 571-305-XXXX
VACANT CELL: XXX-XXX-XXXX

ASSISTANT DIRECTOR (b)(6)
(b)(6)

SENIOR POLICY ADVISOR (b)(6)
(b)(6)

STATE DEPARTMENT REPRESENTATIVE (b)(6)
(b)(6)

DEPUTY UNDER SECRETARY DEFENSE INTEL (b)(6)
(b)(6)

JOINT STAFF CCICA (b)(6)
(b)(6)

22A PROGRAM DIRECTION

DEPUTY ASSISTANT DIRECTOR (b)(6)
(b)(6)

SENIOR PROGRAM ANALYST (b)(6)
(b)(6)

FOR OFFICIAL USE ONLY
PAGE 1

22DEC15

SUBJ: NCIS-2/NATIONAL SECURITY DIRECTORATE KEY PERSONNEL DATA SHEET

DIVISION CHIEF (b)(6)
(b)(6)

SUPERVISORY SPECIAL AGENT PROGRAMS/POLICY (b)(6)
(b)(6)

FPD PROGRAM MANAGER OFFICE: (b)(6)
(b)(6)

FOSO (b)(6)
(b)(6)

22B INVESTIGATIONS

DEPUTY ASSISTANT DIRECTOR (b)(6)
(b)(6)

DIVISION CHIEF (b)(6)
(b)(6)

NCIS REP. TO NAVSEA 08 (Naval Reactors) (b)(6)
(b)(6)

SUPERVISORY SPECIAL AGENT INV (b)(6)
(b)(6)

DIVISION CHIEF INSIDER THREAT (b)(6)
(b)(6)

SUPERVISORY SPECIAL AGENT INSIDER THREAT (b)(6)
(b)(6)

LNO N2N6 (b)(6)
(b)(6)

NJTTF DEPUTY UNIT CHIEF (b)(6)
(b)(6)

STAFF PSYCHOLOGIST (b)(6)
(b)(6)

22C OPERATIONS

DEPUTY ASSISTANT DIRECTOR (b)(6)
(b)(6)

DIVISION CHIEF, IRREG/RDA WARFARE (b)(6)
(b)(6)

SUPERVISORY SPECIAL AGENT RDA (b)(6)
(b)(6)

22DEC15

SUBJ: NCIS-2/NATIONAL SECURITY DIRECTORATE KEY PERSONNEL DATA SHEET

DIVISION CHIEF, OPERATIONS (b)(6)
(b)(6)

SUPERVISORY SPECIAL AGENT OPS OFFICE: XXX-XXX-XXXX
VACANT CELL: XXX-XXX-XXXX

SR. NCIS REP, OUSN, DUSN (b)(6)
(b)(6)

DIVISION CHIEF, SENSITIVE PRO. INTIGRATION (b)(6)
(b)(6)

22D CYBER & DEFENSE CRITICAL INFRASTRUCTURE PROTECTION

DIVISION CHIEF PROGRAMS (b)(6)
(b)(6)

SUPERVISORY SPECIAL AGENT (b)(6)
(b)(6)

CYBER TECH PROGRAM MANAGER OFFICE: 571-305-XXXX
VACANT CELL: XXX-XXX-XXXX

COMPUTER LAW AND NATIONAL SECURITY (b)(6)
(b)(6)

NCIS REP TO CYBERCOM J2X (b)(6)
(b)(6)

NCIS REP TO FCC/C10F (b)(6)
(b)(6)

NCIS REP TO FBI NCIJTF (b)(6)
(b)(6)

22 ANALYTIC DIVISION

SUPERVISORY INTELLIGENCE SPECIALIST (b)(6)
(b)(6)

SUPERVISORY INTELLIGENCE SPECIALIST (b)(6)
(b)(6) CELL:

22 LEGAL DIVISION

FOR OFFICIAL USE ONLY
PAGE 3

22DEC15

SUBJ: NCIS-2/NATIONAL SECURITY DIRECTORATE KEY PERSONNEL DATA SHEET

NATIONAL SECURITY LAW (b)(6)
(b)(6)

FOR OFFICIAL USE ONLY
PAGE 4 LAST (b)(6)

2351619 12:08 20160203 IN:SSDEMAIL #4 OUT:NCISWWSSD #3

GENERAL ADMINISTRATION 03FEB16

FROM: NFNF GEN: NF-0002

TO: DIST

SUBJ: NCIS - 2 (NFNF) NCISRA NORFOLK VA DATA SHEET

PARENT NCISFO: NFFO

NOTE SUBORDINATE OFFICES: NFCE, NFFM, NFHV, NFLC, NFPV, NFYT, NFXA, NFXH, NFXL, NFXO, NFXQ, NFX1, NFX3

NOTE: NCIS OFFICES UNDER NCISRA NORFOLK ARE SERVICED BY THE NCIS CENTRAL EVIDENCE FACILITY (CEF) AND EVIDENCE SHOULD BE MAILED DIRECTLY TO THEM AT: 9079 HAMPTON BLVD, SUITE 110, NORFOLK VA 23505-1098. THE LONG TERM STORAGE (LTS) FACILITY IS STILL PENDING THE TESTING AND IMPLEMENTATION OF AN ELECTRONIC CUSTODY SYSTEM. FURTHER GUIDANCE IS PENDING.

MAILING ADDRESS	LOCAL ADDRESS
NCIS NORFOLK FIELD OFFICE	BLDG U-40
1329 BELLINGER BLVD	NAVAL STATION
NORFOLK VA 23511-2310	NORFOLK VA

TELEPHONES:

OFFICE: (757) 444-7327 DSN: 564
(757) 444-1672 DSN: 564

UNCLAS FAX: (757) 444-3139 DSN: 564

AFTER HOURS:
DUTY TEXT NOTIFICATION: (757) 475-2481

NAVAL BASE:
POLICE WATCH CAPTAIN: (757) 322-2551

NCIS/NLETS ORI: VANIS0900
NMSG PLA: NAVCRIMINSVERFO NORFOLK VA//NFNF//
UIC: 45086

TERRITORIAL COVERAGE: ALL MILITARY INSTALLATIONS (SHORE AND AFLOATS) IN VIRGINIA, LESS THE COUNTIES OF: ARLINGTON, CAROLINE, CLARKE, CULPEPPER, ESSEX, FAIRFAX, FAUQUIER, FREDERICK, GREENE, KING GEORGE, LANCASTER, LOUDOUN, MADISON, NORTHCUMBERLAND, ORANGE, PAGE, PRINCE WILLIAM, RAPPAHANNOCK, RICHMOND COUNTY, ROCKINGHAM, SHENANDOAH, SPOTSYVANIA, STAFFORD, WARREN AND WESTMORELAND.

FOR OFFICIAL USE ONLY
PAGE 1 LAST (b)(6)

1639738 13:19 20150508 IN:SSDEMAIL #1 OUT:NCISWWSSD #1

GENERAL ADMINISTRATION 08MAY15

FROM: 002G GEN: 2G-0002

TO: DIST

SUBJ: NCIS-1/OFFICE OF FORENSIC SUPPORT (OFS) KEY PERSONNEL LISTING

(b)(6)

MAILING AND LOCAL ADDRESS:
Naval Criminal Investigative Service
Office of Forensic Support: 2GFG
Russell-Knox Building
27130 Telegraph Road
Quantico, VA 22134

Vacant
Forensic Consultant
Office Code: 2GFJ
Coverage Area: SEFO, MEFO, CRFO
Mailing Address:
NCIS Southeast Field Office

P.O. Box 58
Jacksonville, FL 32212

(b)(6)

Coverage Areas: FEFO and SNFO
Office Code: 2GFK
Mailing Address:
NCIS Okinawa Japan
Unit 35021

08MAY15

SUBJ: NCIS-1/OFFICE OF FORENSIC SUPPORT (OFS) KEY PERSONNEL LISTING

FPO AP 96373-5021

(b)(6)

Office Coverage: 2GFD
Coverage Area: MWFO
Mailing Address:
NCIS Marine Corps West Field Office
Bldg. 120101 De Luz Road
Camp Pendleton, CA 92055-5238

(b)(6)

Office Code: 2GFW
Coverage Areas: DCFO, NEFO, CRFO
Mailing Address:
NCIS Washington Field Office
2713 Mitscher Road, SW
Bldg. 168, STE 200
Anacostia Annex, DC 20373

(b)(6)

Coverage Areas: NWFO, CNFO
Office Code: 2GFS
Mailing Address:
NCIS Southwest San Diego Field Office
3405 Welles Street
Bldg. 57, STE 1
San Diego, CA 93136-5018

(b)(6)

Office Code: 2GFS
Coverage Area: SWFO
Mailing Address:
NCIS Southwest San Diego Field Office
3405 Welles Street
Bldg. 57, STE 1
San Diego, CA 93136-5018

08MAY15

SUBJ: NCIS-1/OFFICE OF FORENSIC SUPPORT (OFS) KEY PERSONNEL LISTING

(b)(6)

(b)(6)

Office Code: 2GFN
Coverage Areas: NFFO and EUFO
Mailing Address:
NCIS Norfolk Field Office
1329 Bellinger Boulevard
Norfolk, VA 23511

(b)(6)

Office Code: 2GFC
Coverage Areas: CAFO and MEFO
Mailing Address:
NCIS Carolinas Field Office
H32 Julian C. Smith Dr.
Camp Lejeune, NC 28547-1603

(b)(6)

Office Code: 2GFJ
Mailing Address:
NCIS Southeast Field Office
P.O. Box 58
Jacksonville, FL 32212

(b)(6)

Office Code: 2GFL
Coverage Area: SEFO
Mailing Address:
US Army Criminal Investigation Laboratory (USACIL)
4930 N. 31st St, Bldg. 925
Forest Park, GA 30297

Vacant
Forensic Consultant
Office Code: 2GFP
Coverage Area: CNFO

Mailing Address:
NCIS Central Field Office
305 Bronson Ave
Bldg. 2B STE 100

08MAY15

SUBJ: NCIS-1/OFFICE OF FORENSIC SUPPORT (OFS) KEY PERSONNEL LISTING

Great Lakes, IL 60088-2900

(b)(6)

Office Code: 2GFI
Coverage Area: HIFO
Mailing Address:
NCIS Hawaii Field Office
449 South Ave
Bldg. 221
Pearl Harbor, HI 96860-4988

DISTRIBUTION
NCISHQ: All Departments and Directorates
INFO: WWSSD

FOR OFFICIAL USE ONLY
PAGE 4 LAST (b)(6)

1847657 13:35 20150722 IN:SSDEMAIL #8 OUT:NCISWWSSD #4

GENERAL ADMINISTRATION 22JUL15

FROM: 000C GEN: 00C-0038

TO: DIST

SUBJ: NCIS-2 (CODE 00C) COMMUNICATIONS DIRECTORATE DATA SHEET AND KEY PERSONNEL LISTING

PLEASE SEE THE BELOW FOR KEY PERSONNEL LISTING:

Director of Communications, (b)(6)
Office:
Blackb (b)(6)

Public Affairs Officer, (b)(6)
Offic
Cell: (b)(6)

Audiovisual Production Specialist, (b)(6)
Offic
Cell: (b)(6)

Writer/Editor, (b)(6)
Offic
Cell: (b)(6)

Website Content Manager, (b)(6)
Offic
Cell: (b)(6)

Graphic Specialist, (b)(6)
Offic
Cell: (b)(6)

Event Coordinator, (b)(6)
Offic
Cell: (b)(6)

Public Affairs Specialist, (b)(6) effective: 22JUL15)
Office: (b)(6)

Public Affairs Specialist, (b)(6) effective: 10AUG15)
Office: (b)(6)

FOR OFFICIAL USE ONLY
PAGE 1 LAST (b)(6)

1923793 09:35 20150819 IN:SSDEMAIL #1 OUT:NCISWWSSD #1

GENERAL ADMINISTRATION 18AUG15

FROM: 0000 GEN: 0I-0007

TO: DIST

SUBJ: NCIS-2/ (00I) OFFICE OF THE INSPECTOR GENERAL (00I) KEY PERSONNEL LISTING

MAILING ADDRESS/LOCAL ADDRESS
NAVAL CRIMINAL INVESTIGATIVE SERVICE HEADQUARTERS OFFICE OF INSPECTOR GENERAL ATTN: CODE 00I
27130 Telegraph Road W-3170
Quantico, VA 22134-2253

TELEPHONES COMMERCIAL
OFFICE: (571) 305-9O79
AFTER HOURS: NCIS MTAC (571) 305-4777

TITLE	KEY PERSONNEL
Inspector General	(b)(6)
Deputy IG	
Div Chief Investigations	
Div Chief Inspections	

SSA Vacant
Investigations

SSA Inspections

(b)(6)

FOR OFFICIAL USE ONLY
PAGE 1

18AUG15

SUBJ: NCIS-2/ (00I) OFFICE OF THE INSPECTOR GENERAL (00I) KEY PERSON

Investigative Assistant
Inspections Support

(b)(6)

Program Support Assistant
Admin Support

DISTRIBUTION
NCISHQ: All Directorates and Departments
INFO: WWSSD/AFLT

FOR OFFICIAL USE ONLY
PAGE 2 LAST (b)(6)

U.S. NAVAL CRIMINAL INVESTIGATIVE SERVICE

GENERAL ADMINISTRATION 31AUG15

FROM: OOSS GEN: OSS-0004

TO: DISTRIBUTION

SUBJ: NCIS-2 (OSS) OFFICE OF STRATEGIC SUPPORT DATA SHEET

MAILING ADDRESS:
NAVAL CRIMINAL INVESTIGATIVE SERVICE OFFICE OF STRATEGIC SUPPORT
2713 MITSCHER RD SW STE 300
JOINT BASE ANACOSTIA BOLLING DC 20373-5107

TELEPHONES	COMMERICAL	DSN
SAC	(b)(6)	
SSA		
SSA		

* DENOTES STU-III/STE CAPABILITY

UNCLAS//

FOR OFFICIAL USE ONLY

(b)(6)

U.S. NAVAL CRIMINAL INVESTIGATIVE SERVICE

GENERAL ADMINISTRATION
31AUG15

FROM: OOSS

GEN: OSS-0005

TO: DISTRIBUTION

SUBJ: NCIS-2 (OSS) OFFICE OF STRATEGIC SUPPORT KEY PERSONNEL LISTING

MAILING ADDRESS:
NAVAL CRIMINAL INVESTIGATIVE SERVICE OFFICE OF STRATEGIC SUPPORT
12713 MITSCHER RD SW STE 300
JOINT BASE ANACOSTIA BOLLING, DC 20373-5107

(b)(6)

2. POC at OSS is (b)(6)

DISTRIBUTION
NCISHQ: ALL DEPARTMENT AND DIRECTORATES
INFO: WWSSD

FOR OFFICIAL USE ONLY

(b)(6)

WARNING

THIS DOCUMENT IS THE PROPERTY OF THE NAVAL CRIMINAL INVESTIGATIVE SERVICE CONTENTS MABY BE DISCLOSED ONLY TO PERSONS WHOSE OFFICIAL DUTIES REQUIRE ACCESS HERE TO CONTENTS MAY NOT BE DISCLOSED TO THE PARTY(S) CONCERNED WITHOUT SPECIFIC AUTHORIZATION FROM THE NAVAL CRIMINAL INVESTIGATIVE SERVICE

2302896 14:10 20160120 IN:SSDEMAIL #14 OUT:NCISWWSSD #6

GENERAL ADMINISTRATION 20JAN16

FROM: 2GTQ GEN: 02G-0002

TO: DIST

SUBJ: NCIS-2: OFFICE OF TECHNICAL SERVICES KEY PERSONNEL DATA SHEET

MAILING ADDRESS
Naval Criminal Investigative Service HQ
Office of Technical Services (OTS)(2GTQ) Russell-Knox Building
27130 Telegraph Road
Quantico, VA 22134-2253

TITLE/PERSONNEL CONTACT NUMBERS

(b)(6)

NCIS Norfolk Detachment (2GTV)
1801 Tomcat Blvd, Bldg 321
Virginia Beach, VA 23460-2289

(b)(6)

NCIS San Diego Detachment (2GTC)
3405 Welles Street
Bldg 57 Suite 1
San Diego, CA 92136

(b)(6)

(b)(6)

Field Operations Support Officer

(b)(6)

DISTRIBUTION

FOR OFFICIAL USE ONLY
PAGE 1

20JAN16

SUBJ: NCIS-2: OFFICE OF TECHNICAL SERVICES KEY PERSONNEL DATA SHEET

NCISHQ: All Departments and Directorates
INFO: WWSSD

FOR OFFICIAL USE ONLY
PAGE 2 LAST (b)(6)

2306077 08:13 20160121 IN:SSDEMAIL #1 OUT:NCISWWSSD #1

GENERAL ADMINISTRATION 21JAN16

FROM: 2GTQ GEN: 02G-0003

TO: DIST

SUBJ: NCIS-2: OFFICE OF TECHNICAL SERVICES DATA SHEET

MAILING ADDRESS
Naval Criminal Investigative Service HQ
Office of Technical Services Department (OTSD) Russell-Knox Building
27130 Telegraph Road
Quantico, VA 22134-2253

Telephones	Commercial	DSN
Office:	(571) 305-9177	240
Unclas Facsimile:	(571) 305-9085	
After Hours: NCIS MTAC	(571) 305-4777	

NMSG PLA: DIRNAVCRIMINVSERV Quantico VA/2GTQ// NCIC/NLETS ORI: None
UIC: 63285
Electrical Distribution: /2GTQ/

NCISTSD WASHINGTON (2GTS)
Co-Located With NCISHQ Code 2GTQ

Telephones	Commercial	DSN
Office:	(571) 305-9177	240
Unclas Facsimile:	(571) 305-9085	
After Hours: NCIS MTAC	(571) 305-4777	

Territorial Coverage:
District of Columbia; Virginia; Counties of Arlington; Fairfax, Loudoun, Accomack, Culpeper, Fauquier, Prince, William, Spotsylvania, Stafford, King George, Northampton, Westmoreland, Richmond, Lancaster, Essex, and Caroline, Orange, Green, Madison, Rockingham, Page, Rappahannock, Warren, Clarke, Frederick, and Shenandoah; Cities of Alexandria, Falls Church, Fairfax, Vienna, and Fredericksburg; State of Maryland.

DETACHMENTS:

NCISTSD Camp Lejeune (2GTD)
Mailing/Local Address
H-32 Julian C. Smith Drive
Camp Lejeune, NC 28547-1603

Telephones	Commercial	DSN
Office:	(910) 449-6516/4385	752
Unclas Facsimile:	(910) 449-6505	

FOR OFFICIAL USE ONLY

21JAN16

SUBJ: NCIS-2: OFFICE OF TECHNICAL SERVICES DATA SHEET

NCIC/NLETS ORI: NCNIS 0200
UIC: 35626 (CALE)

Territorial Coverage:
All Counties in North and South Carolina.

NCISTSD Hawaii (2GTH)

Mailing/Local Address	Local Address
449 South Avenue	452 Bailey Street
Pearl Harbor, HI 96860-4988	Camp Smith, Hi 96861

Telephones	Commercial	DSN
Office:	(808)447-0010/0021	315
Unclas Facsimile:	(808) 447-0025	

PLA: NAVCRIMINVSERV TECHSVC DET Pearl Harbor HI//2GTH// NCIC/NLETS ORI: None
UIC: 35630 (HIHN)

Territorial Coverage:
The State Of Hawaii (Including Oahu, Maui, Hawaii And Kauai Counties) Midway Island, Kingman Reef, Phoenix Islands, American Samoa, Baker Island, Cook Island, Daner Island, French Polynesia Islands, Howard Island, Johnston Island, Line Islands, Midway Island, Niue Island, Phoenix Islands, Pitcaim Islands, Tokelau Islands, Society Islands, Tuamotu Archipelago, Tubuai Islands, Western Samoa, Northern Marianas Islands, Federated States Of Micronesia, Republic Of Palau, Republic of the Marshall

Islands, Tokelau Islands, Society Islands, Tuamotu Archipelago, Marquesas Islands, Antarctica, Guam, Marianas Islands, Australia, New Zealand, Japan, Okinawa, Korea, Philippines, and Singapore.

NCISTSD Bahrain (2GTB)
Mailing/Local Address Local/Delivery Address (FEDEX,UPS,DHL)
PSC 851 Box 520 DLA Distribution Bahrain, Southwest Asia
FPO AE 09834-0006 GENCO Logistics Park, Bahrain Investment
Warf (BIW),RD 1527 Plot #A36(Bldg 1978),
Al Hidd 115, Kingdom of Bahrain

Telephones	Commercial	DSN
Office:	011-973-1785-4392	318
Unclas Facsimile:	011-973-1785-4116	

Territorial Coverage:
The Middle East, Arabian Peninsula, Arabian Gulf, Gulf Of Aden, Gulf Of Oman, The Red Sea, and the Islands of Mauritius and Seychelles.

The Middle East Countries Specifically Covered Are:
Bahrain, Egypt, Iran, Jordan, Kazakhstan, Kuwait, Kyrgyzstan, Lebanon, Mauritius, Oman, Pakistan, Qatar, Saudi Arabia, Seychelles,

21JAN16

SUBJ: NCIS-2: OFFICE OF TECHNICAL SERVICES DATA SHEET

Syria, Tajikistan, Turkmenistan, United Arab Emirates, Uzbekistan, Yemen

NCISTSD Norfolk (2GTV)
Mailing/Local Address
1801 Tomcat Blvd
Bldg 321, Virginia Beach, VA 23460

Telephones	Commercial	DSN
Office:	(757) 433-3885	433
Unclas Facsimile:	(757) 433-3949	

PLA: NAVCRIMINVSERV TECH SVC DET Norfolk VA//2GTV//
UIC: 63055

Territorial Coverage: All Military Installations (Shore and Afloat) in Virginia, less the Counties of: Arlington, Caroline, Clarke, Culpeper, Essex, Fairfax, Fauquier, Frederick, Greene, King George, Lancaster, Loudoun, Madison, Northumberland, Orange, Page, Prince William, Rappahannock, Richmond, Rockingham, Shenandoah, Spotsylvania, Stafford, Warren and Westmoreland.

NCISTSD Bangor (2GTG)
Mailing/Local Address
1003 Sunfish Drive
Silverdale, WA 98315

Telephones	Commercial	DSN
Office:	(360) 396-4408/7195	744
Unclas Facsimile:	(360) 396-4424	

PLA: NAVCRIMINVSERV TECH SVC DET Bangor WA//2GTG//
UIC: 42951 (NWBG)

Territorial Coverage:
Alaska, California: All Counties, north of, and including, San Luis Obispo, King and Inyo. Washington, Oregon, Idaho, Montana, Utah, Colorado, Wyoming, Northern Nevada.

NCISTSD Jacksonville (2GTM)

Mailing Address	Local/Delivery Address (FedEx, Ups)
Po Box 58	Building 875, 1st Floor
Naval Air Station	Allegheny Road
Jacksonville, FL 32212-0058	NAS Jacksonville, FL 32212

Telephones	Commercial	DSN
Office:	(904) 542-2684/5369	542
Unclas Facsimile:	(904)542-8631	

NMSG PLA: DIRNAVCRIMINVSERVFO Southeast Mayport FL//2GTM// NCIC/NLETS ORI: None

21JAN16

SUBJ: NCIS-2: OFFICE OF TECHNICAL SERVICES DATA SHEET

UIC: 42933 (SEFO)

Territorial Coverage:
Providing Technical Support to the Southeast Field Office and parts of Gulf Coast Field Office. Areas Of Responsibility (AOR) include Alabama, Arkansas, Florida, Georgia, Louisiana, Mississippi, Oklahoma, Tennessee, and Texas. All Counties except El Paso, Hudspeth and Culberson; South America and the Caribbean.

NCISTSD San Diego (2GTC)
Mailing Address
3405 Welles Street
Bldg 57 Suite 1
San Diego, CA 92136

Telephones	Commercial	DSN
Office:	(619) 524-0613/0605	524
Unclas Facsimile:	(619) 524-0618	

NMSG PLA: DIRNAVCRIMINSERV TECHSVC DET San Diego CA//2GTC// NLETS/NCIC ORI: Caniso400
UIC: 42943

Territorial Coverage:
Arizona: All Counties
California: All Counties
Nevada: Clark Counties
New Mexico: All Counties
Oklahoma: All Counties
Texas: All Counties
El Paso: All Counties
Hudspeth: All Counties
Culberson: All Counties
South America and the Caribbean.

NCISTSD Europe and Africa

Mailing Address	Local Address
PSC 812 Box 3360	Bldg 469
FPO AE 09627-3360	US Naval Air Station
	NAS Sigonella (II)
	95100 Catania, Sicily, IT

Telephones	Commercial	DSN
From Conus:	011-39-095-86-9264	314
Within Italy:	095-86-9264	

Within Europe: 0039-095-86-9264

The above office is not manned on a continuous basis, please contact HQ if no one responds. 571-305-9177.

21JAN16

SUBJ: NCIS-2: OFFICE OF TECHNICAL SERVICES DATA SHEET

Note: For technical support for Europe/Africa AOR please send leads to NCISHQ Code 2GTQ.

Territorial Coverage: Continent of Europe and all Littoral Areas, United Kingdom, Iceland, Turkey and Israel. Continent of Africa (except for Egypt and the Islands of Seychelles and Mauritius).

FOR OFFICIAL USE ONLY
PAGE 5 LAST (b)(6)

2214538 11:51 20151214 IN:SSDEMAIL #16 OUT:NCISWWSSD #16

GENERAL ADMINISTRATION 14DEC15

FROM: SEFO GEN: SE-0032

TO: DIST

SUBJ: 53342035MH.DOC - *CORRECTED COPY* NCIS-2 (SEAU/CNAU) NCISRU
AUSTIN TX DATA SHEET

**********CI COVERAGE ONLY**********

PARENT NCISFO: SOUTHEAST FIELD OFFICE MAYPORT FL (SEFO) PARENT NCISRA: PENSACOLA FL (SEPF/CNPF)

NOTE: NCISRU AUSTIN TX is no longer under the ADCON/OPCON of Central Field Office as of 01NOV15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNAU, assigned to NCISRU AUSTIN TX, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code SEAU/NCISRU AUSTIN TX will not be used until NJIS comes online. Please copy SEFO/CNPF, as appropriate. All other correspondence will utilize SEAU.

MAILING ADDRESS AND LOCAL ADDRESS:
FEDERAL BUREAU OF INVESTIGATION
TFO TROY NOBLE, CI-2
12515-7 RESEARCH BLVD FBI
SUITE 400 SUITE 400
AUSTIN, TX 78759 AUSTIN, TX 78759

TELEPHONES COMMERCIAL ONLY
OFFICE 512-506-4111
CELL PHONE 512-731-4719
UNCLAS FAX 512-506-2686 (USE COVER SHEET)

SSD TELECOMMS
NMSG PLA: NAVCRIMINVSERVRA AUSTIN TX
NCIC/NLET ORI: NONE
UIC: N34416

TERRITORIAL COVERAGE: CI/RTP/CE LEADS ONLY. ALL GENCRIM/FRAUD/CBT LEADS SHOULD BE DIRECTED TO SECC/CNCC, SESO/CNSO, OR SEDA/CNDA (SEE NCIS 2 FOR AOR).

TEXAS: ALL COUNTIES EXCEPT FOR EL PASO, HUDSPETH, REEVES AND CULBERTSON.
OKLAHOMA: ALL COUNTIES
KANSAS: ALL COUNTIES
PRINCIPAL INSTALLATION SERVICED:
UNIVERSITY OF TEXAS, APPLIED RESEARCH LABORATORY, AUSTIN, TX

**********CI COVERAGE ONLY**********

FOR OFFICIAL USE ONLY
PAGE 1 LAST (b)(6)

2214363 10:47 20151214 IN:SSDEMAIL #11 OUT:NCISWWSSD #11

GENERAL ADMINISTRATION 14DEC15

FROM: SEFO GEN: SE-0024

TO: DIST

SUBJ: NCIS-2 (SECC/CNCC) NCISRU CORPUS CHRISTI TX DATA SHEET

PARENT NCISFO: SOUTHEAST FIELD OFFICE (SEFO) PARENT NCISRA: DALLAS TX (SEDA/CNDA)

NOTE: NCISRU CORPUS CHRISTI TX is no longer under the ADCON/OPCON control of Central Field Office as of 01NOV15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNCC, assigned to NCISRU CORPUS CHRISTI TX, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code SECC/NCISRU CORPUS CHRISTI TX will not be used until NJIS comes online. Please copy SEFO/CNDA, as appropriate. All other correspondence will utilize SECC.

MAILING ADDRESS LOCAL ADDRESS
385 FIFTH ST SE SUITE 2A BUILDING 39
CORPUS CHRISTI, TX 78419-5034 NAVAL AIR STATION
CORPUS CHRISTI TX 78419-5034

TELEPHONES	COMMERCIAL	DSN PREFIX
OFFICE	(361) 961-2918/2919/2839	861
UNCLAS FAX	(361) 961-2429	861
SECURE FAX	(b)(6)	

OMNI (STE): (361) 961-1374 (SSA) 861
OMNI (STE): (361) 961-1372 (SIPRNET RM) 861 AFTER HOURS: (361) 597-0001 SSA CELL

SSD TELECOMMUNICATIONS: NIPRNET
NMSG PLA: NAVCRIMINVSERVREP CORPUS CHRISTI TX NCIC/NLET ORI: NONE
UIC: 42936
BASE STATION IDENTIFIER CODE (NFC): 1181

TERRITORIAL COVERAGE:
THE FOLLOWING COUNTIES: ANGELINA; ARANSAS; AUSTIN; BEE; BROOKS; BRAZORIA; BURLESON; CALHOUN; CAMERON; CHAMBERS; COLORADO; DEWITT; DUVAL; FORT BEND; GALVESTON; GOLIAD; GRIMES; HARDIN; HARRIS; HILDALGO; HOUSTON; JACKSON; JASPER; JEFFERSON; JIM HOGG; JIM WELLS; LIVE OAK; KENEDY; KLEBERG; LIBERTY; MATAGORDA; MCMULLEN; MONTGOMERY; NEWTON; NUECES;

ORANGE; POLK; REFUGIO; SAN JACINTO; SAN PATRICIO; TRINITY; TYLER; VICTORIA; WALKER; WALLER; WHARTON; WILLACY;

PRINCIPAL INSTALLATION SERVICED:
CNATRA NAS KINGSVILLE NOSC HARLINGEN
TRAWING TWO NAS CORPUS CHRISTI NOSC CORPUS CHRISTI TRAWING FOUR MATSG CORPUS CHRISTI
VT-21 MCRD HOUSTONVT-22 NRD HOUSTON

FOR OFFICIAL USE ONLY
PAGE 1

14DEC15

SUBJ: NCIS-2 (SECC/CNCC) NCISRU CORPUS CHRISTI TX DATA SHEET

VT-27 PSA CORPUS CHRISTI
VT-28 NAVRESCEN HOUSTON
VT-31 NAVRESCEN CORPUS CHRISTI
VT-35 PSA CORPUS CHRISTI

FOR OFFICIAL USE ONLY
PAGE 2 LAST (b)(6)

2224330 08:23 20151217 IN:SSDEMAIL #1 OUT:NCISWWSSD #1

GENERAL ADMINISTRATION 17DEC15

FROM: SEFO GEN: SE-0035

TO: DIST

SUBJ: *CORRECTED COPY" NCIS-2 (SEDA/CNDA) NCISRA DALLAS TX DATA SHEET

PARENT NCISFO: SOUTHEAST FIELD OFFICE MAYPORT FL (SEFO) SUBORDINATE NCISRU: SESO/CNSO, SECC/CNCC, SEOC/CNOC

NOTE: NCISRA DALLAS TX is no longer under the ADCON/OPCON control of Central Field Office as of 01NOV15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNDA, assigned to NCISRA DALLAS TX, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code SEDA/NCISRA DALLAS TX will not be used until NJIS comes online. Please copy SEFO, as appropriate. All other correspondence will utilize SEDA.

MAILING AND LOCAL ADDRESS
1701 E. LAMAR BLVD STE 292
ARLINGTON, TX 76011

TELEPHONES COMMERCIAL ONLY
OFFICE (817) 860-5260
UNCLAS FAX (817) 860-2394
AFTER HOURS NAS JRB FORT WORTH, TX (817) 782-5200 SECURITY DISPATCH

DMS PLA: NAVCRIMINVSERVRA DALLAS TX
NCIS-CNFO ORI: ILNIS1000
UIC: 34415

TERRITORIAL COVERAGE
THE FOLLOWING COUNTIES: ANDERSON; ANDREWS; ARCHER; ARMSTRONG; BAILEY; BAYLOR; BELL; BORDEN; BOSQUE; BOWIE; BRAZOS; BRISCOE; BROWN; CALLAHAN; CAMP; CARSON; CASS; CASTRO; CHEROKEE; CHILDRESS; CLAY; COCHRAN; COKE; COLEMAN; COLLIN; COLLINGSWORTH; COMANCHE; CONCHO; COOKE; CORYELL; COTTLE; CRANE; CROSBY; DALLUM; DALLAS; DAWSON; DEAF SMITH; DELTA; DENTON; DICKINS; DONLEY; EASTLAND; ECTOR; ELLIS; ERATH; FALLS; FANNIN; FISHER; FLOYD; FOARD; FRANKLIN; FREESTONE; GAINES; GARZA; GLASSOCK; GRAY; GRAYSON; GREGG; HALE; HALL; HAMILTON;

HANSFORD; HARDEMAN; HARRISON; HARTLEY; HASKELL; HEMPHILL; HENDERSON; HILL; HOCKLEY; HOOD; HOPKINS; HOWARD; HUNT; HUTCHINSON; JACK; JOHNSON; JONES; KAUFMAN; KENT; KING; KNOX; LAMAR; LAMB;LAMPASAS; LEON; LYPSCOMB; LIMESTONE; LUBBOCK; LOVING; LYNN; MCCLENNAN; MADISON; MARION; MARTIN; MIDLAND; MILLS; MITCHELL; MONTAGUE; MOORE; MORRIS; MOTLEY; NACOGDOCHES; NAVARRO; NOLAN; OCHILTREE; OLDHAM; PALO PINTO; PANOLA; PARKER; PARMER; POTTER; RAINS; RANDALL; RED RIVER; !
REEVES; ROBERTS; ROCKWALL; RUNNELS; RUSK; SABINE; SAN AUGUSTINE; SCURRY; SHACKELFORD; SHELBY; SHERMAN; SMITH; SOMERVELL; STEPHENS;

FOR OFFICIAL USE ONLY
PAGE 1

17DEC15

SUBJ: *CORRECTED COPY" NCIS-2 (SEDA/CNDA) NCISRA DALLAS TX DATA SHEE

STERLING; STONEWALL; SWISHER; TARRANT; TAYLOR; TERRY; THROCKMORTON; TITUS; TOM GREEN; UPSHUR; VAN ZANDT; WARD; WHEELER; WINKLER; WITCHITA; WILBARGER; WISE; WOOD; YOAKUM; YOUNG;

PRINCIPAL INSTALLATIONS SERVICED
NAS JRB FT WORTH 8TH MARINE RECRUITING DISTRICT 14TH MARREG NAVCRUITDIST DALLAS
COMFLELOGSUPPWING NAVPRO DALLAS COMNAVRESINTEL COMM NORTHRUP/GRUMMAN AIRCORP
NOCD DALLAS DCMA DALLAS REGION VMFA-112
VR-59 VR-6
MAG-41 NAVAL OPERATION SUPPORT CENTER (NOSC)
MACS-24 FLEET READINESS CENTER (FRC) WEST
MWSS-473 BRANCH MEDICAL CLINIC

FOR OFFICIAL USE ONLY
PAGE 2 LAST (b)(6)

2214379 10:52 20151214 IN:SSDEMAIL #13 OUT:NCISWWSSD #13

GENERAL ADMINISTRATION 14DEC15

FROM: SEFO GEN: SE-0029

TO: DIST

SUBJ: NCIS-2 (SEGF/CNGF) NCISRA GULFPORT MS DATA SHEET

PARENT NCISFO: SOUTHEAST FIELD OFFICE MAYPORT FL (SEFO) SUBORDINATE NCISRU: MERIDIAN (SEMJ/CNMJ), NEW ORLEANS (SENR/CNNR)

NOTE: NCISRA GULFPORT MS is no longer under the ADCON/OPCON control of Central Field Office as of 01OCT15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNGF, assigned to NCISRA GULFPORT MS, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code SEGF/NCISRA GULFPORT MS will not be used until NJIS comes online. Please copy SEFO/CNPF, as appropriate. All other correspondence will utilize SEGF.

MAILING AND LOCAL ADDRESS
NCBC BLDG 109
2208 BARRY AVENUE
GULFPORT MS 39501

TELEPHONES	COMMERCIAL	DSN PREFIX
OFFICE	(228) 871-2211	868
UNCLAS FAX	(228) 871-3068	868
AFTER HOURS SECURITY	(228) 871-2361	868

NMSG PLA: NAVCRIMINVSERVRA GULFPORT MS
NCIC/NLETS ORI: NONE
UIC: 34413

TERRITORIAL COVERAGE:
MISSISSIPPI - THE FOLLOWING COUNTIES:
HARRISON, HANCOCK, JACKSON, PEARL RIVER, STONE, GEORGE, GREENE, PERRY, FORREST, LAMAR, MARION, WALTHALL, PIKE, AMITE, WILKINSON, ADAMS, FRANKLIN, LINCOLN, LAWRENCE, JEFFERSON DAVIS, COVINGTON, JONES, WAYNE, CLARKE, JASPER, SMITH SIMPSON, COPIAH, JEFFERSON, AND CLAIBORNE

ALABAMA - THE FOLLOWING COUNTIES:
MOBILE, WASHINGTON, CLARKE, CHOCTAW, MARENGO, SUMTER, GREENE, AND HALE

PRINCIPAL INSTALLATIONS SERVICED:
CBC GULFPORT; RESERVE NAVAL CONSTRUCTION FORCE; NCG2; NAVAGATIONAL AIDS SUPPORT UNIT; NMCB-1; NMCB-11; NMCB 74; NMCB 133; INSPECTOR-INSTRUCTOR STAFF (USMC); STENNIS SPACE CENTER, NAVOCEANO; NAVAL RESEARCH LABORATORY DETACHMENT; COMNAVOCEANCOM; AVOCEANOCOMFAC; SPECIAL BOAT UNIT TWENTY-TWO; CHIEF OF NAVAL METEOROLOGICAL AND OCEANOGRAPHY COMMAND (CNMOC); NAVAL OCEANOGRAPHY ASW CENTER; NAVAL

14DEC15

SUBJ: NCIS-2 (SEGF/CNGF) NCISRA GULFPORT MS DATA SHEET

SMALL CRAFT INSTRUCTION AND TECHNICAL TRAINING SCHOOL (NAVSCIATTS); NAVAL FLEET SURVEY TEAM; NAVAL METEOROLOGY AND OCEANOGRAPHY PROFESSIONAL DEVELOPMENT CENTER (PDC) SOUTH; NAVY HUMAN RESOURCES SERVICE CENTER SOUTHEAST.

FOR OFFICIAL USE ONLY
PAGE 2 LAST (b)(6)

2214391 10:55 20151214 IN:SSDEMAIL #15 OUT:NCISWWSSD #15

GENERAL ADMINISTRATION 14DEC15

FROM: SEFO GEN: SE-0031

TO: DIST

SUBJ: NCIS-2 (SEMJ/CNMJ) NCISRU MERIDIAN MS DATA SHEET

PARENT NCISFO: SOUTHEAST FIELD OFFICE MAYPORT FL (SEFO) PARENT NCISRA: GULFPORT MS (SEGF/CNGF)

NOTE: NCISRU MERIDIAN MS is no longer under the ADCON/OPCON of Central Field Office as of 01OCT15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNMJ, assigned to NCISRU MERIDIAN MS, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code SEMJ/NCISRU MERIDIAN MS will not be used until NJIS comes online. Please copy SEFO/CNPF, as appropriate. All other correspondence will utilize SEMJ.

MAILING AND LOCAL ADDRESS
NCISRU MERIDIAN
255 ROSENBAUM AVENUE
ROOM 134
MERIDIAN MS 39309

TELEPHONES	COMMERCIAL	DSN PREFIX
OFFICE	(601) 679-2564	637
UNCLAS FAX	(601) 679-2060	637
AFTER HOURS SECURITY	(601) 679-2361	637

DMS PLA: NAVCRIMINVSERVRA GULFPORT MS
NCIC/NLETS ORI: NONE
UIC: 67980

TERRITORIAL COVERAGE:
MISSISSIPPI: ALL COUNTIES NORTH OF INTERSTATE 20:
WARREN, HINDS, RANKIN, SCOTT, NEWTON, LAUDERDALE, KEMPER, NESHOBA, LEAKE, MADISON, YAZOO, SHARKEY, ISSAQUENA, WASHINGTON, HUMPHREYS, HOLMES, ATTALA, WINSTON, NOXUBEE, LOWNDES, OKTIBBEHA, CHOCTAW, MONTGOMERY, CARROLL, LEFLORE, SUNFLOWER, BOLIVAR, TALLAHATCHIE, GRENEDA, WEBSTER, CLAY MONROE, CHICKASAW, CALHOUN, YALOBUSHA, COAHOMA, QUITMAN, PANOLA, LAFAYETTE, UNION, PONTOTOC, LEE, ITAWAMBA, TISHOMINGO, PRENTISS, ALCORN, TIPPAH, BENTON, MARSHALL, TATE, TUNICA AND DESOTO.

ALABAMA: THE FOLLOWING COUNTIES:

PICKENS, TUSCALOOSA, JEFFERSON, ST. CLAIR, CALHOUN, CLEBURNE, CHEROKEE, ETOWAH, BLOUNT, WALKER, FAYETTE, LAMAR, MARION, WINSTON, CULLMAN, FRANKLIN, COLBERT, LAUDERDALE, LAWRENCE, MORGAN, LIMESTONE, MADISON, JACKSON, MARSHALL AND DEKALB

PRINCIPAL INSTALLATIONS SERVICED:

14DEC15

SUBJ: NCIS-2 (SEMJ/CNMJ) NCISRU MERIDIAN MS DATA SHEET

NAS MERIDIAN, TRAINING AIR WING ONE, NTTC, MATSS-1, NOSC, FAA, CNATRA DETACHMENT MERIDIAN, NAFC

FOR OFFICIAL USE ONLY
PAGE 2 LAST (b)(6)

2214240 10:23 20151214 IN:SSDEMAIL #3 OUT:NCISWWSSD #3

GENERAL ADMINISTRATION 14DEC15

FROM: SEFO GEN: SE-0028

TO: DIST

SUBJ: NCIS-2 (SEMT/CNMT) NCISRU MEMPHIS DATA SHEET

PARENT NCISFO: SOUTHEAST FIELD OFFICE MAYPORT FL (SEFO) PARENT NCISRA: ST LOUIS MO (SESL/CNSL)

NOTE: NCISRU MEMPHIS TN is no longer under the ADCON/OPCON control of Central Field Office as of 01NOV15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNMT, assigned to NCISRU MEMPHIS TN, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code SEMT/NCISRU MEMPHIS TN will not be used until NJIS comes online. Please copy SEFO/CNSL, as appropriate. All other correspondence will utilize SEMT.

MAILING ADDRESS	LOCAL ADDRESS (USE FOR FEDEX/UPS)
NCISRU MEMPHIS	NCISRU MEMPHIS
5722 INTEGRITY DRIVE	7700 HORNET AVE
MILLINGTON, TN 38054-5058	BLDG 455, 3RD FLOOR
	MILLINGTON, TN 38054-5058

TELEPHONES	COMMERCIAL	DSN
OFFICE:	(901)874-5387/89	882-5387
UNCLAS FAX:	(901)874-5218	882-5218
FCI STE:	(901)874-6247	882-6247

AFTER HOURS (SECURITY): (901)832-6177 (WATCH COMMANDER)

NMSG PLA: NAVCRIMINVSERVREP MEMPHIS TN
NCIC/NLETS ORI: NONE
UIC: 42937
BASE STATION IDENTIFIER CODE: NFC 656

TERRITORIAL COVERAGE
TENNESSEE - ALL COUNTIES
ARKANSAS - ALL COUNTIES

PRINCIPAL INSTALLATIONS SERVICED:
NAVY PERSONNEL COMMAND (NPC); NAVY RECRUITING COMMAND (NRC); NSA MID-SOUTH; DECA COMSY MEMPHIS, TN; NBHC MID-SOUTH; DPRO; MWRTU (WASHINGTON); NAVCRUITDIST MEMPHIS, TN; NAVMAC MEMPHIS, TN; PERSUPP DET MEMPHIS, TN; US AIR FORCE DET 2/CC (361TRS); USN & MCRTC KNOXVILLE, TN; NOSC MILLINGTON, TN; NOSC NASHVILLE, TN; NOSC KNOXVILLE, TN; NOSC CHATTANOOGA, TN; NOSC LITTLEROCK, AR.

2214382 10:53 20151214 IN:SSDEMAIL #14 OUT:NCISWWSSD #14

GENERAL ADMINISTRATION 14DEC15

FROM: SEFO GEN: SE-0030

TO: DIST

SUBJ: NCIS-2 (SENR/CNNR) NCISRU NEW ORLEANS LA DATA SHEET

PARENT NCISFO: SOUTHEAST FILED OFFICE MAYPORT FL (SEFO) PARENT NCISRA: GULFPORT MS (SEGF/CNGF)

NOTE: NCISRU NEW ORLEANS LA is no longer under the ADCON/OPCON of Central Field Office as of 01OCT15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNNR, assigned to NCISRU NEW ORLEANS LA, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code SENR/NCISRU NEW ORLEANS LA will not be used until NJIS comes online. Please copy SEFO/CNGF, as appropriate. All other correspondence will use SENR.

MAILING AND LOCAL ADDRESS
400 RUSSELL AVE
BLDG 557
NEW ORLEANS LA 70143

TELEPHONES	COMMERCIAL	DSN PREFIX
OFFICE	(504) 678-2257	678
UNCLAS FAX	(504) 678-3968	678
AFTER HOURS SECURITY	(504) 678-3333	678

DMS PLA: NAVCRIMINVSERVREP NEW ORLEANS LA NCIC/NLET ORI: NONE BASE STATION IDENTIFIER CODE: NFC 650
UIC: 42938

TERRITORIAL COVERAGE:
LOUISIANA: ALL PARISHES

PRINCIPAL INSTALLATIONS SERVICED: CG MARINE FORCES RESERVES; CG FOURTH MARINE AIR WING; CG FOURTH MARINE DIVISION; GC FOURTH MARINE LOGISTICS GROUP; MILITARY ENTRANCE PROCESSING STATION NEW ORLEANS; MILITARY SEALIFT COMMAND SURGE DETACHMENT NEW ORLEANS; NAVY AIR LOGISTICS OFFICE, NAVY RECRUITING DISTRICT NEW ORLEANS; NAVAL

AMBULATORY CARE CENTER NEW ORLEANS; NAVY RESERVE PROFESSIONAL DEVELOPMENT CENTER NEW ORLEANS; NAVY BAND NEW ORLEANS; NAVSUPPACT NEW ORLEANS; SUPSHIP GULF COAST NEW ORLEANS; SPAWARSYSCEN NEW ORLEANS; NAS JRB NEW ORLEANS; FLEET READINESS CENTER MID-ATLANTIC SITE NEW ORLEANS; NAVAL OPERATIONAL SUPPORT CENTER NEW ORLEANS; STRIKE FIGHTER SQUADRON 204 (VFA-204) NEW ORLEANS; FLEET LOGISTICAL SUPPORT SQUADRON 54 (VR-54) NEW ORLEANS; AIRBORN EARLY MORNING SQUAD (VAW-77) NEW ORLEANS; MARINE AIRCRAFT GROUP 49; DETACHMENT C NEW ORLEANS; 3RD BATTALION 23RD MARINES 4TH MARDIV NEW ORLEANS; NAVY AIR LOGISTIC

14DEC15

SUBJ: NCIS-2 (SENR/CNNR) NCISRU NEW ORLEANS LA DATA SHEET

OFFICE NEW ORLEANS

2214374 10:50 20151214 IN:SSDEMAIL #12 OUT:NCISWWSSD #12

GENERAL ADMINISTRATION 14DEC15

FROM: SEFO GEN: SE-0026

TO: DIST

SUBJ: NCIS-2 (SEOC/CNOC) NCISRU OKLAHOMA CITY OK DATA SHEET

PARENT NCISFO: SEFO
PARENT NCISRA: SEDA/CNDA

NOTE: NCISRU OKLAHOMA CITY OK is no longer under the ADCON/OPCON control of Central Field Office as of 01NOV15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNOC, assigned to NCISRU OKLAHOMA CITY OK, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code SEOC/NCISRU OKLAHOMA CITY OK will not be used until NJIS comes online. Please copy SEFO/CNDA, as appropriate. All other correspondence will utilize SECC.

MAILING AND LOCAL ADDRESS
AFOSI DET 114 TINKER AFB OK
ATTN: NCIS
3540 C AVENUE, BLDG 3
TINKER AFB, OK 73145-9114

TELEPHONES	COMMERCIAL	DSN
OFFICE:	202-421-0518	NONE
RESIDENT AGENT	202-421-0518	

DMAS PLA: NAVCRIMINVSERVRA DALLAS TX
NCIC/NLETS ORI: NONE
UIC: 34486

TERRITORIAL COVERAGE:
OKLAHOMA (ALL COUNTIES)
KANSAS (ALL COUNTIES)

PRINCIPAL INSTALLATIONS SERVICED:
CNAT; VQ-3; VQ-4; VQ-7

2214247 10:28 20151214 IN:SSDEMAIL #4 OUT:NCISWWSSD #4

GENERAL ADMINISTRATION 14DEC15

FROM: SEFO GEN: SE-0019

TO: DIST

SUBJ: NCIS-2 (SEPA/CNPA) NCISRU PASCAGOULA MS DATA SHEET

PARENT NCISFO: SOUTHEAST FIELD OFFICE MAYPORT FL (SEFO) PARENT NCISRA: JACKSONVILLE FL (SEJX - FRAUD)

NOTE: NCISRU PASCAGOULA MS is no longer under the ADCON/OPCON of Central Field Office as of 01OCT15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNPA, assigned to NCISRU PASCAGOULA MS, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code SEPA/NCISRU PASCAGOULA MS will not be used until NJIS comes online. Please copy SEFO/SEJX, as appropriate. All other correspondence will utilize SEPA.

MAILING ADDRESS: LOCAL ADDRESS
PO BOX 1652 535 DELMAS AVE STE 23
PASCAGOULA MS 39568-1652 PASCAGOULA MS 39567

TELEPHONES COMMERCIAL DSN
OFFICE (228) 769-4455 457-4455
UNCLAS FAX (228) 769-2743 457-2743
AFTER HOURS SECURITY (228) 871-2361 868-2361

DMS PLA: NAVCRIMINVSERVREP PASCAGOULA MS NCIC/NLETS ORI: NONE
UIC: 34414

TERRITORIAL COVERAGE:
ONLY MAJOR PROCUREMENT FRAUD INVESTIGATIONS/LEAD COVERAGE IN THE STATES OF MISSISSIPPI AND ALABAMA.

MISSISSIPPI: ALL COUNTIES

ALABAMA: MOBILE COUNTY AND ALL COUNTIES SOUTH OF INTERSTATE 20 EXCEPT BARBOUR, COFFEE, COVINGTON, CRENSHAW, DALE, GENEVA, HENRY, HOUSTON AND PIKE.

PRINCIPAL INSTALLATIONS SERVICED:
SUPSHIP GULF COAST PASCAGOULA, MS; INGALLS SHIPBUILDING PASCAGOULA, MS; BAE SHIPBUILDING, MOBILE, AL; AUSTAL SHIPBUILDING, MOBILE, AL; LITTORAL COMBAT SHIP PRECOMM UNITS AUSTAL USA MOBILE, AL.

2214267 10:37 20151214 IN:SSDEMAIL #7 OUT:NCISWWSSD #7

GENERAL ADMINISTRATION 14DEC15

FROM: SEFO GEN: SE-0022

TO: DIST

SUBJ: NCIS-2 (SEPC/CNPC) NCISRU PANAMA CITY FL DATA SHEET

PARENT NCISFO: SOUTHEAST FIELD OFFICE MAYPORT FL (SEFO) PARENT NCISRA: NCISRA PENSACOLA FL (SEPF/CNPF)

NOTE: NCISRU PANAMA CITY FL is no longer under the ADCON/OPCON of Central Field Office as of 01OCT15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNPC, assigned to NCISRU PANAMA CITY FL, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code SEPC/NCISRU PANAMA CITY FL will not be used until NJIS comes online. Please copy SEFO/CNPF, as appropriate. All other correspondence will utilize SEPC.

MAILING ADDRESS LOCAL ADDRESS
NAVAL SUPPORT ACTIVITY NAVAL SUPPORT ACTIVITY
101 VERNON AVE. BLDG 304 BLDG 304, ROOM 124
PANAMA CITY BEACH, FL 32407-7018

TELEPHONES COMMERCIAL DSN
OFFICE (850) 234-4306 436-4306/5695
UNCLAS FAX (850) 234-4857 436-4857
SECURE PHONE (850) 235-5695 436-5695
AFTER HOURS (SECURITY) (850) 234-4332 436-4332

NMSG PLA: NAVCRIMINVSERVREP PANAMA CITY FL NCIC/NLET ORI: NONE
UIC: 34412

TERRITORIAL COVERAGE
ALABAMA: COUNTIES OF BARBOUR, COFFEE, COVINGTON, CRENSHAW, DALE, GENEVA, HENRY, HOUSTON, PIKE, RUSSELL

FLORIDA: COUNTIES OF BAY, CALHOUN, FRANKLIN, GADSEN, GULF, HOLMES, JACKSON, LIBERTY, WAKULLA, WALTON AND WASHINGTON

PRINCIPAL INSTALLATIONS SERVICED:
NAVAL SUPPORT ACTIVITY PANAMA CITY, NAVAL SURFACE WARFARE CENTER NSWC), PANAMA CITY, NAVY EXPERIMENTAL DIVING UNIT (NEDU), CENTER FOR EOD AND DIVING, NAVY DIVING AND SALVAGE

TRAINING CENTER (NDSTC), EOD GROUP TWO DETACHMENT, FSD NROTC FLORIDA A&M UNIVERSITY, TALLAHASSEE, NAVRESCEN TALLAHASSEE

FOR OFFICIAL USE ONLY
PAGE 1 LAST (b)(6)

2221650 10:57 20151216 IN:SSDEMAIL #2 OUT:NCISWWSSD #2

GENERAL ADMINISTRATION 16DEC15

FROM: SEFO GEN: SE-0034

TO: DIST

SUBJ: *CORRECTED COPY* NCIS-2 (SEPF/CNPF) NCISRA PENSACOLA FL DATA SHEET

PARENT NCISFO: SOUTHEAST FIELD OFFICE MAYPORT FL (SEFO) SUBORDINATE NCISRU: AUSTIN TX (SEAU/CNAU); PANAMA CITY FL (SEPC/CNPC); FPD COLOMBIA (SECB); FPD HONDURAS (SETH); FPD GUATEMALA (SEGG)/ FPD EL SALVADOR (SESS)

NOTE: NCISRA PENSACOLA FL is no longer under the ADCON/OPCON of Central Field Office as of 01OCT15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNPF, assigned to NCISRA PENSACOLA FL, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code SEPF/NCISRA PENSACOLA FL will not be used until NJIS comes online. Please copy SEFO, as appropriate. All other correspondence will utilize SEPF.

NCISRA MAILING ADDRESS
821 SAN CARLOS ROAD
BUILDING 3813
NAVAL AIR STATION
PENSACOLA FL 32508-5133

LOCAL ADDRESS (CRIM/CT)	LOCAL ADDRESS (CI)
821 SAN CARLOS ROAD	544 THOMPSON AVE
BUILDING 3813	BUILDING 544
NAVAL AIR STATION	CORRY STATION
PENSACOLA FL 32508-5133	PENSACOLA FL 32511

TELEPHONES	COMMERCIAL	DSN PREFIX
OFFICE (CRIM/CT)	(850) 452-4211	459
OFFICE (CI)	(850) 452-6081	459
UNCLAS FAX (CRIM/CT)	(850) 452-4282	459
UNCLAS FAX (CI)	(850) 452-6193	459

(b)(6)

SSA (CRIM/CT/CI) (850) 452-4211 459
AFTER HOURS - DUTY AGENT VIA NAS SECURITY DEPT
(850) 452-3453/2453 459

NMSG PLA: NAVCRIMINVSERVRA PENSACOLA FL NCIC/NLETS ORI: ILNIS1020
UIC: 67556

TERRITORIAL COVERAGE
ALL ALABAMA COUNTIES FOR CRIM AND CI/CT

FOR OFFICIAL USE ONLY
PAGE 1

16DEC15

SUBJ: *CORRECTED COPY* NCIS-2 (SEPF/CNPF) NCISRA PENSACOLA FL DATA S

PRINCIPLE INSTALLATIONS SERVED:
NAS PENSACOLA; NAVAL AEROSPACE MEDICAL INSTITUTE (NAMI);NAVAL AEROSPACE MEDICAL RESEARCH LABORATORY (NAMRL); NAVAL AIR TECHNICAL TRAINING CENTER (NATTC); MARINE AVIATION TRAINING SUPPORT GROUP 21 (MATSG-21); NAVAL AVIATION SCHOOLS COMMAND (NASC); NAVAL EDUCATION AND TRAINING COMMAND (NETC); NAVAL EDUCATION TRAINING AND SECURITY ASSISTANCE FIELD ACTIVITY (NETSAFA); NAVAL HOSPITAL PENSACOLA, NAVAL LEGAL SERVICE OFFICE CENTRAL (NLSOC); REGION LEGAL SERVICE OFFICE SOUTHEAST DETACHMENT PENSACOLA; TRAWING-6; NAVAL OPERATION MEDICINE INSTITUTE (NOMI) HQ; NAVY FLIGHT DEMONSTRATION SQUADRON (BLUE ANGELS); VT-4; VT-10; VT-86; CENTER FOR INFORMATION DOMINANCE; CORRY STATION; NIOC PENSACOLA; SAUFLEY FIELD; NAVAL EDUCATION AND TRAINING PROFESSIONAL DEVELOPMENT AND TECHNOLOGY CENTER (NETPDTC); NAS WHITING FIELD MILTON FL; TRAWING-5; NAVAL SCHOOL EXPLOSIVE ORDNANCE DISPOSAL (NAVSCHOLEOD) AT EGLIN AFB

2214217 10:21 20151214 IN:SSDEMAIL #2 OUT:NCISWWSSD #2

GENERAL ADMINISTRATION 14DEC15

FROM: SEFO GEN: SE-0018

TO: DIST

SUBJ: NCIS-2 (SESL/CNSL) NCISRA ST LOUIS MO DATA SHEET

PARENT NCISFO: SOUTHEAST FIELD OFFICE MAYPORT FL (SEFO) SUBORDINATE NCISRU: SEMT/CNMT, SEDA/CNDA (FRAUD ONLY)

NOTE: NCISRA ST LOUIS MO is no longer under the ADCON/OPCON of Central Field Office as of 01NOV15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNSL, assigned to NCISRA ST LOUIS MO, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code SESL/NCISRA ST LOUIS MO will not be used until NJIS comes online. Please copy SEFO/CNMT, as appropriate. All other correspondence will utilize SESL.

MAILING ADDRESS LOCAL ADDRESS
NCISRA ST LOUIS NCISRA ST LOUIS
1 ARCHIVES DRIVE SUITE 350 1 ARCHIVES DRIVE SUITE 350
ST LOUIS, MO 63138 ST LOUIS, MO 63138

TELEPHONES COMMERCIAL NO DSN AVAILABLE
OFFICE: (314)538-2323/4
UNCLAS FAX: (314)538-2325
AFTER HOURS: (314)686-2367 (DUTY CELLPHONE)

**********NO SIPRNET CAPABILITY**********

NMSG PLA: NAVCRIMINSERVRA ST LOUIS MO
NCIC/ NLETS ORI: NONE
UIC: 34418

TERRITORIAL COVERAGE:
MISSOURI: ALL COUNTIES
ILLINOIS: SOUTHERN AREA
ADDITIONALLY: RECORD INQUIRIES FOR THE NATIONAL PERSONNEL RECORDS CENTER (NPRC) AND VETERANS AFFAIRS OFFICE

PRINCIPAL INSTALLATIONS SERVICED:
NATIONAL PERSONNEL RECORDS CENTER (NPRC), ST LOUIS, MO; FORT LEONARDWOOD, MO; MCDONNELL-BOEING CORP, ST LOUIS, MO; MARCORCRUITSTA, ST LOUIS, MO; NOSC ST LOUIS, MO; NOSC SPRINGFIELD, MO; NOSC KANSAS CITY, MO; NOSC CAPE GIRARDEAU, MO; NROTCU, COLUMBIA, MO; SCOTT AIR FORCE BASE, IL

FOR OFFICIAL USE ONLY
PAGE 1 LAST (b)(6)

2214329 10:45 20151214 IN:SSDEMAIL #10 OUT:NCISWWSSD #10

GENERAL ADMINISTRATION 14DEC15

FROM: SEFO GEN: SE-0027

TO: DIST

SUBJ: NCIS-2 (SESO/CNSO) NCISRA SAN ANTONIO DATA SHEET

PARENT NCISFO: SEFO
PARENT NCISRA: SEDA/CNDA

NOTE: NCISRU SAN ANTONIO TX is no longer under the ADCON/OPCON control of Central Field Office as of 01NOV15. Currently, Consolidated Law Enforcement Operations Center (CLEOC) still identifies the code of CNSO, assigned to NCISRU SAN ANTONIO TX, and will be used for reporting purposes when using CLEOC. Upon implementation of the Naval Justice Information System (NJIS), the new office code SEC0/NCISRU SAN ANTONIO TX will not be used until NJIS comes online. Please copy SEFO/CNDA, as appropriate. All other correspondence will utilize SESO.

MAILING ADDRESS	LOCAL ADDRESS
OFFICE OF SPECIAL INVESTIGATIONS	OFFICE OF SPECIAL INVESTIGATIONS
ATTN: NCIS	ATTN: NCIS
2170 KENLY AVE	2170 KENLY AVE
LACKLAND AFB TX 78236	LACKLAND AFB TX 78236

TELEPHONES	COMMERCIAL	DSN
OFFICE	NONE	NONE
CELL PHONE	(361) 799-1157	
	(361) 533-7656	
UNCLAS FAX	(210) 671-4764 (PLEASE USE FAX COVER SHEET)	
SECURE FAX	NONE	

NMSG PLA: NAVCRIMINVSERVRA DALLAS TX
NCIS/NLET ORI NONE
UIC: 67981

TERRITORIAL COVERAGE:
MAJOR CITIES INCLUDE: SAN ANTONIO, AUSTIN, DEL RIO, EAGLE PASS, GEORGETOWN, SAN MARCOS, BRYAN, LAREDO

THE FOLLOWING COUNTIES: ATACOSA; BANDARA; BASTRUP; BEXAR; BLANCO; BREWSTER; CALDWELL; COMAL; CROCKET; DIMMIT; EDWARDS; FAYETTE; FRIO; GILLESPIE; GONZALES; GUADALUPE; HAYS; IRION; KENDALL; KERR; KIMBLE; KINNEY; LA SALLE; LAVACA; LEE; LLANO; MASON; MAVERICK;

MCCULLOCH; MEDINA; MILAM; PECOS; REAGAN; REAL; ROBERTSON; SAN SABA; SCHLEICHER; STARR; SUTTON; TRAVIS; UPTON; UVALDE; VAL VERDE; WASHINGTON; WILSON; WEBB; ZAPATA; ZAVALA

PRINCIPAL INSTALLATION SERVICED: NIOC SAN ANTONIO; NTTC DET SAN ANTONIO; NAVRESCEN SAN ANTONIO; NAVRESCEN AUSTIN; 4TH RECON BN; 4TH MARDIV; NRD SAN ANTONIO; NAVMEDTRACEN SAN ANTONIO; NOSC AUSTIN, TX;

14DEC15

SUBJ: NCIS-2 (SESO/CNSO) NCISRA SAN ANTONIO DATA SHEET

NOSC SAN ANTONIO, TX; H CO, MCSB MTEC; RANDOLPH AFB DLI; LACKLAND AFB; NSGA MEDINA SAN ANTONIO; MCRD SAN ANTONIO

1693857 16:08 20150529 IN:SSDEMAIL #8 OUT:NCISWWSSD #8

GENERAL ADMINISTRATION 28MAY15

FROM: SWND GEN: ND-0011

TO: DIST

SUBJ: **CORRECTED COPY**NCIS-2: (SWXE) NCISREP USS ESSEX (LHD 2)
DATA SHEET

ADCON: SWXE OPCON: SWXE

Mailing Address:
NCISREP USS ESSEX (LHD 2)
ATTN SAA (b)(6)
USS ESSEX (LHD 2)
FPO AP 96643-1661

NMSG PLA: NAVCRIMINVSERVREP XRAY ECHO//SWXE (PENDING)

The NCIS agent assigned to USS Essex (LHD 2) is Special Agent Afloat (b)(6) who will provide criminal, force protection, counterterrorism and counterintelligence support to all serviced commands. Send all leads to SWXE with an info copy to SWND.

Commands Serviced:
COMPHIBRON THREE (CPR-3)
USS ESSEX (LHD 2)
USS ANCHORAGE (LPD 23)
USS RUSHMORE (LSD 47)
15TH MARINE EXPEDITIONARY UNIT (15TH MEU)

(b)(6)

DISTRIBUTION
NCISHQ: ALL DEPARTMENTS AND DIRECTORATES
INFO: WWSSD

FOR OFFICIAL USE ONLY
PAGE 1 LAST (b)(6)

Naval Criminal Investigative Service
Managers' Internal Control (MIC) Plan

This plan is reviewed annually.

Last Update: September 2015

MIC Senior Official: Director, NCIS

The Director is the senior official within NCIS and reports to the Under Secretary of the Navy.

MIC Coordinator: NCIS Inspector General (IG)

The IG reports to the Director, NCIS. Assignments to this position are generally for 3-5 years. Duties as MIC Coordinator are on a part-time basis.

Alternate MIC Coordinator: Inspections Division Chief, NCIS Inspector General

The alternate MIC coordinator reports to the MIC Coordinator/NCIS Inspector General. Assignments to this position are generally for 3-5 years. Duties as alternate MIC coordinator are on a part-time basis.

Overview of the MIC Plan within the Organization:

Control Environment

Mission

The NCIS mission is to conduct criminal, counterintelligence, terrorism related investigations and operations, and to provide security services as delineated in SECNAVINST 5430.107. In short, the NCIS mission is to "Prevent Terrorism, Protect Secrets and Reduce Crime."

Strategic Plan

The current NCIS Strategic Plan provides the overarching strategy for the organization. Director's guidance and program direction documents provide annual goals and objectives. An updated long term strategic plan is in development.

Organizational Structure

NCIS senior leadership is organized into a headquarters element, consisting of the Director, Deputy Director, Principal Executive Assistant Director for Management and Administration (PEAD), 6 Executive Assistant Directors, programmatic Deputy Assistant Directors, Special Agents In Charge and 13 field offices. Areas of responsibility for field elements are delineated in the NCIS-2 Office Directory.

The internal controls (IC) reporting chain follows established organizational lines of authority from assessable units to the Executive Assistant Director (EAD)/Assistant Director (AD) level and then to the MIC coordinator. Addendum 1 provides an inventory of assessable units and assessable unit managers.

Funding within NCIS flows from the comptroller to EADs/ADs and Deputy Assistant Directors (DAD) at NCIS headquarters and geographic EADs to Special Agents In Charge (SACs) at field offices who are provided annual budgets to execute their assigned functions.

Risk Assessment

NCIS leaders and the MIC coordinator conduct risk assessments throughout the year to identify assess and prioritize control risks associated with accomplishing the NCIS mission. Results of self-inspections, management visits, audits, inspections, monitoring of programs, inquiries and investigations, are reviewed to identify risk.

Control Activities

NCIS program managers are responsible for identifying and developing appropriate control activities to ensure the accomplishment of assigned missions. Control activities are documented in NCIS manuals, policy documents, instructions, field office performance plans, and in this MIC Plan. In some instances there are two levels of control activities in a specific risk area, one in the field and one in NCIS headquarters. NCIS program managers are responsible for monitoring their programs in conjunction with field office leadership and with the NCIS IG to ensure control activities are not just appropriate for the activity, but are being exercised as intended. The MIC senior management official may also order spot checks/control assessments for specific activities that affect the NCIS organization and mission.

Information and Communications

Information is communicated via four primary means:

- General administration messages (GENADMIN) are used to communicate guidance, changes in policy, procedures, and to provide situational awareness.
- NCIS manuals and instructions are used to document NCIS policy and procedures, and are posted on the NCIS Lighthouse intranet portal. Operational reporting is disseminated via Reports of Investigation transmitted via Naval Justice Information System (NJIS), SIPRnet, or NIPRnet.
- E-mail is used to disseminate information and taskers to targeted audiences. The weekly News to You is used to disseminate general information to a NCIS-wide audience. The NCIS administration and logistics directorate utilizes e-mail to disseminate items in the NCIS tasker system.
- Program and field office performance plans and reviews are used to convey performance expectations and to track significant issues.

Monitoring

Control Activities

The major types of monitoring activities within NCIS are:

- Field Office Management Visits: Each field office element will be visited on a semi-annual basis by a senior manager in accordance with policy per NCIS-1, Chapter 5 (Inspector General Matters).
- Quality Assurance Visits (QAV): Geographic EADs will form teams to conduct annual visits, to each field office to review investigations and operations to assess the quality and timeliness of these products.
- Headquarters Case Review: NCIS headquarters operational departments will review Special Interest (SI), Director's Special Interest (DSI) investigations and operations to ensure the quality and timeliness of these products.
- Self-Inspections: Each assessable unit manager will conduct a self-inspection annually in accordance with NCIS-1, Chapter 5. Beginning this year, the self-inspection will include one internal control assessment.
- NCIS IG Inspections: The NCIS IG will conduct cyclical inspections for each field office, STAATLANT and STAATPAC and headquarter departments.
- Naval Audits: The Naval Audit Service will regularly review special operations funds and Emergency and Extraordinary Expense Funds (E&EE) expenditures.
- Assistant to the Secretary of Defense (Intelligence Oversight) (ATSD (10)) Visits: The ATSD (IO) conducts random site visits to ensure NCIS activities are in compliance with DoD 5240.1-R, law, and other policies.
- Audits/Inspections: The Government Accounting Office, DoD Inspector General, Naval Inspector General, and Naval Audit Service conduct periodic inspections and audits of NCIS activities.
- Monthly supervisory case review (SCRS) has been established to evaluate and quality control on all pending investigative cases from all the NCIS field offices.
- Geographic EAD management staffs will conduct random case review/quality control for investigations conducted by their respective field offices. They will also conduct similar reviews for cases they designate as "Special Interest".

Each assessable unit is required to conduct one internal control assessment during the year and to report the results along with the results of the annual self-inspection directed in NCIS-1, Chapter 5.

Accomplishments

NCIS management utilizes U.S. Navy and U.S. Marine Corps strategies and requirements by developing a program direction document (PDD) to develop strategic direction and goals for each operational program: National Security Division (NSD), Criminal Investigative, Directorate of Intelligence and Information Sharing (DIIS), Cyber and Global Operations. The NCIS field offices use the PDD's to develop NCIS field tactical plans.

Program directors are responsible for tracking individual program accomplishments and metrics in concert with the NCIS performance planning cycle. NCIS program assessment and evaluation continues to improve. Performance measures are used by program directors to help monitor the impact of their respective programs, and to help identify performance gaps for any one performance year. NSD performance measures are classified and posted on the SIPRnet. Specific performance measures for Global Operations and DIIS are being developed.

Corrective Action Plans

The NCIS IG/MIC coordinator identifies significant control deficiencies during internal and external audits, inspections, headquarters control assessments and self-assessments, and follows up to ensure corrective action plans are implemented. In addition to internal tracking tools, the Department of the Navy (DON) Statement of Assurance Tool is used to track major deficiencies. Assessable unit managers are responsible for self-reporting control deficiencies identified during management visits and external inspections/audits, developing corrective action plans, and implementing corrective actions in a timely manner.

MIC Training

MIC coordinators and alternates are required to complete the MIC program training. Managers of assessable units will complete MIC Program Training for Managers. Training will be refreshed every three years. Addendum 2 provides a course description and procedures for accessing these online courses.

Reporting Requirements

NCIS Resident Agencies (NCISRA's) will report the results of self-assessments to their respective field offices by 31 March of each year. Assessable unit managers will report results of self-assessments and internal control assessments to the MIC Coordinator by 30 April. The MIC coordinator and EAD for Financial Management and Planning will brief the results of self-assessments, performance reviews, and material weaknesses to the Director and executive staff by 30 June.

Risk Assessment Documentation/Risk Assessment Table

The risk assessment table is reviewed annually.

Control Assessment Documentation

NCIS internal controls are a fluid and continual process. NCIS managers must actively assess risk and evaluate internal controls to ensure the controls are balanced and are effectively mitigating the associated risks. Control assessments will include both an internal review of controls, and evaluations from external organizations, such as audit organizations or higher level offices of Inspector General.

Every manager of an assessable unit will conduct at least one internal control assessment each year. The annual internal assessment may be specified by the MIC senior management official.

During the risk assessment, controls were rated as having a low, moderate, or high control risk. If a control risk is determined to be high, there is no need to test the control. The reason for not testing the controls labeled "high" is that those controls have not been implemented, or are not effective in either their design or operation, and therefore must be improved. Corrective action plans will be developed for all controls that are rated as having high control risk.

Controls with low or moderate control risk should be monitored and/or occasionally tested to see if the controls are effective. If the control is assessed to be ineffective, the control should be reconsidered. Corrective action plans should be developed for those controls that are not effective.

Significant control deficiencies should be reported to the NCIS MIC coordinator as either a reportable condition or material weakness based on management judgment. A material weakness is a major control deficiency requiring senior Navy influence to resolve.

While internal control assessment documentation is required, there is no prescribed format for completing an internal control assessment for the MIC program overall. The goal is to maintain internal control assessment documentation that gives managers the information they need to establish and improve internal controls within their command.

Corrective Action Plans

Managers are to:

- Promptly evaluate findings from audits and other reviews, including those showing deficiencies and recommendations reported by auditors and others who evaluate agencies' operations.
- Determine proper actions in response to findings and recommendations from audits and reviews.
- Complete actions to correct or otherwise resolve matters brought to management's attention.

The resolution process begins when audit or other review results are reported to management, and is completed only after action has been taken that corrects identified deficiencies, produces improvements, or demonstrates that findings and recommendations do not warrant management action.

Corrective action plans for all material weaknesses and reportable conditions will be an enclosure to the NCIS MIC Certification Statement.

Addendum 1

Inventory of Assessable Units

Assessable Unit Name	Assessable Unit Manager
Headquarters Elements	
00C – Office of Communication	AD
00F – Comptroller	DAD
00I – Inspector General	AD
00L – Office of General Counsel	Counsel
01AM – Office of Military Support (OMS)	CO
02A – Atlantic Operations	EAD
02G – Global Operations	EAD
02P – Pacific Operations	EAD
10A – Human Resources Operations and Services	AD
10B – Training Department	DAD
10D – Human Capital Development Department	DAD
11A – Security and Facilities Department	DAD
11B – Acquisition and Logistics Department	DAD
11C – Administrative Services	DAD
14 – Strategic Planning	Comptroller
15 – Information Technology	EAD
22 – National Security Directorate	EAD
23 – Criminal Investigations	EAD
25 – Intelligence and Information Sharing	AD

Assessable Unit Names	Assessable Unit Manager
Field Offices	
CAFO – Carolina Field Office	SAC
CBFO – Cyber Field Office	SAC
CNFO – Central Field Office	SAC
CRFO – Contingency Response Field Office	RAC
DCFO – Washington Field Office	SAC
EUFO – Europe and Africa Field Office	SAC
FEFO – Far East Field Office	SAC
HIFO – Hawaii Field Office	SAC
MEFO – Middle East Field Office	SAC
MWFO – Marine West Field Office	SAC
NEFO – Northeast Field Office	SAC
NFFO – Norfolk Field Office	SAC
NWFO – Northwest Field Office	SAC
OPS – Office of Polygraph Services	SAC
OSP – Office of Special Projects	SAC
OSS – Office of Strategic Support	SAC
POFO – Protective Operations Field Office	SAC
SEFO – Southeast Field Office	SAC
SNFO – Singapore Field Office	SAC
STAAT LANT – STAAT Atlantic	STAAT CDR
STAAT PAC – STAAT Pacific	STAAT CDR
SWFO – Southwest Field Office	SAC

Addendum 2

Managers' Internal Control (MIC) Training

MIC training is available online through Navy e-Learning and Navy Knowledge Online. The information below provides an explanation of the two courses and information on how to access the courses.

DON MIC Program Training for Coordinators

About the Course
The purpose of the course is to provide an overview of the DON MIC Program. It is designed for MIC coordinators and alternates with management control responsibilities for their units in the DON. This course meets the training requirement for MIC coordinators per SECNAVINST 5200.35E.

Content
This course is divided into five modules, which introduce the basic definitions and concepts related to the DON MIC Program, and provide more detailed explanations and examples where necessary.

Objectives
After completing this course participants should be able to:

- Explain the fundamentals of management controls.
- Understand DON MIC Program requirements and responsibilities.
- Describe how to use tools and techniques to evaluate and enhance a MIC Program.
- Describe the DON Statement of Assurance process.

Estimated Duration
Completion time for this course is approximately seven hours.

DON MIC Training for Managers

About the Course
The purpose of this course is to provide DON Managers with a foundation for understanding internal controls and the DON MIC Program. This course is designed for managers and does not meet SECNAVINST 5200.35E training requirements for MIC coordinators or their alternates.

Content
Course content consists of a single module that is divided into four topics and a module test. These topics introduce basic definitions and concepts related to the DON MIC Program, and provide more detailed explanations and examples where necessary.

Objectives
Objectives of this course are to provide an understanding of:

- Internal controls and their importance.
- The purpose of a MIC.
- DON MIC requirements and responsibilities.

Estimated Duration
Completion time for this course is approximately two hours.

Accessing the Computer Based Training Courses
MIC courses are available through the Navy Knowledge Online website.

To access the courses, go to www.nko.navy.mil.

We recommend that you review the "Get Started" section for detailed directions on accessing and taking courses.

Below is the detailed course information.

Course Title	Catalog Code	Learning Category
Managers' Internal Control Program Training	OASN-MCPT-1	US Department of the Navy (DON)/ Management Control Program
Managers' Internal Control Program Training for Managers	OASN-MCPM-1	US Department of the Navy (DON)/ Management Control Program

Addendum 3

Risk Assessment

Risk Assessment					
Command: Naval Criminal Investigative Service					
#	Risk	Inherent Risk	Control Risk	Combined Risk	Internal Control Currently in Place
1	Investigations are not timely or complete when closed and disseminated to NCIS customers	High	Moderate	Moderate	Monthly Supervisory Case Review; Supervisory release of ROI's
2	PCS related allowances and expenses are incorrectly paid	High	Moderate	Moderate	Review by HQ administrative staff and comptroller
3	Personally Identifiable Information media is lost	Moderate	Moderate	Moderate	Controls are monitored during IG Inspections
4	Timekeeping, Payroll and Allowances - SLDCADA, RSO, Post Differential, Danger Pay, COLA, Leave, Locality Pay are incorrectly paid	Moderate	Moderate	Moderate	Supervisors approve SLDCADA biweekly, NCIS - wide control assessment
5	DTS/TDY travel are not cost effective	Moderate	Moderate	Moderate	Field Office/ HQ/Comptroller reviews/approvals
6	Firearms and/or ammunition are not accounted for	Moderate	Moderate	Moderate	Annual inventory
7	EEE funds are not expended properly	Moderate	Moderate	Low	Monthly cash counts, SAC approval of expenditures, NAVAUDSVC biennial reviews and IG monthly audit
8	Information is improperly collected on U.S. Persons	Moderate	Low	Low	First line supervisory review and annual training requirement
9	Voyager cards are misused	Moderate	Moderate	Moderate	Monthly APC reviews
10	Unsuitable employees are sent overseas requiring early costly return	Moderate	Moderate	Low	Code 10 review
11	Hiring and suitability process is not dependable	Moderate	Moderate	Low	HR administration, 2A, 2S, 2M

12	Employees misuse government vehicles	Moderate	Moderate	Moderate	Logs and reviews and IG Inspections
13	Evidence is improperly handled and stored	Moderate	Moderate	Low	IG Inspections; Annual self-inspection; and Field Office management visits
14	Employees use Government travel cards for unauthorized purchases and fail to pay bills in a timely manner	High	Low	Low	APC's review transactions and delinquent accounts
15	DPAS property accountability is not current	Moderate	Moderate	Moderate	Code 11B review and IG Inspections