Description of document:	Naval Criminal Investigative Service (NCIS) manual 3, 2008
Requested date:	14-December-2015
Released date:	29-September-2016
Posted date:	17-October-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/16U1573
SEP 29 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 a partial release. The processing of the NCIS 3 manual and final release 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) and (b)(7)(C). Exemption (b)(7)(E) has 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 90 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.

If you choose not to appeal, you have the right to seek dispute resolution services. You may contact the Department of the Navy's FOIA public liaison, Mr. Chris Julka, at christopher.a.julka@navy.mil or (703) 697-0031 or the Office of Government Information Services (https://ogis.archives.gov/).

There are no assessable fees associated with the processing of your request. 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, JAGC, USN

Encl:
(1) CD/Documents

CHAPTER 1
TITLE: AUTHORITY, JURISDICTION, AND SCOPE
POC: CODE 00L
DATE: MAY 08

1-1. ESTABLISHMENT OF NCIS

The Naval Criminal Investigative Service (NCIS) was formally established in January 1993 under the Secretary of the Navy. Its predecessor, the Naval Investigative Service (NIS), was established in February 1966 under the Chief of Naval Operations. NCIS is a federal law enforcement agency that protects and defends the Department of the Navy (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 (UCMJ), assists commands in maintaining good order and discipline, and provides law enforcement and security services to the Navy and Marine Corps on a worldwide basis. NCIS had several predecessor organizations with essentially the same mission.

1-2. COUNTERINTELLIGENCE MISSION

1-2.1. NCIS is the primary agency within the DON for the conduct of counterintelligence (CI) and related activities. This responsibility is detailed in SECNAVINST 5430.107 dated 28 December 2005, various Department of Defense (DoD) Directives, and an agreement with the Department of Justice (DOJ) governing the conduct of DoD CI activities. SECNAVINST 3850.2C implements DoD guidance regarding CI functions and restates NCIS responsibility for the conduct of CI for DON, less those combat related CI matters within the functional responsibilities of the Marine Corps.

1-2.2. Definition. Joint Publication 1-02, “DoD Dictionary of Military and Associated Terms”, states that CI investigations are conducted to prove or disprove an allegation of espionage or other intelligence activities, such as sabotage, assassination, or other national security crimes conducted by or on behalf of a foreign government, organization, or person or international terrorists. CI investigations may establish the elements of proof for prosecution or administrative actions, provide a basis for CI operations, or validate the suitability of personnel for access to classified information. CI investigations are conducted against individuals or groups for committing major security violations, as well as failure to follow defense agency and military service directives governing reporting contacts with foreign citizens and out-of-channel requests for defense information. CI investigations provide military commanders and policymakers with information used to eliminate security vulnerabilities and otherwise improve

the security posture of threatened interests.

1-2.3. Objectives. The objectives of DoD and DON CI are, as found in DoD Directive 5240.2 of May 22, 1997 to detect, identify, assess, exploit, and counter or neutralize the intelligence collection efforts, other intelligence activities, sabotage, terrorist activities, and assassination efforts of foreign powers, organizations, or persons directed against DON, its personnel, information, and activities. Within DON, NCIS has exclusive jurisdiction in noncombat matters involving actual, potential, or suspected terrorism, sabotage, espionage, and subversive activities, per SECNAVINST 5430.107. This jurisdiction includes actual, suspected, or attempted defection by DON personnel.

1-3. LIAISON

Within the DON, NCIS has exclusive responsibility for liaison with federal, state, local, and foreign law enforcement, security and intelligence agencies on all criminal investigative, CI, counterterrorism, and security matters assigned to NCIS by SECNAVINST 5430.107 and its references. Commands may pursue interaction with federal, state, local, and foreign law enforcement, security, and intelligence agencies on antiterrorism matters, but shall do so in coordination with NCIS. Execution of this responsibility shall not limit any of the following:

a. Contact between Navy and Marine Corps judge advocates and federal, state or local officials to determine prosecutorial jurisdiction and grants of immunity, coordinate pretrial agreements, or take any other action consistent with the duties of judge advocates.

b. Interaction between commands and federal, state, local, or foreign law enforcement and security officials on routine matters involving physical security, minor offenses, purely military offenses, traffic matters, and training.

c. Liaison conducted by Marine Corps CI elements in accordance with SECNAVINST 3850.2C.

1-4. SECURITY MATTERS

1-4.1. Per SECNAVINST 5510.36 series, coordination between commands and NCIS in security matters will take place immediately in the following circumstances:

a. Classified information has been, or is suspected of being lost, compromised, or subjected to compromise.

b. Request is submitted through other than official channels for classified national defense information from anyone, or for unclassified information from an individual believed to be in contact with a foreign intelligence service.

c. A member with access to classified information commits suicide or attempts to commit suicide.

d. A member who had access to classified information is an unauthorized absentee, and there are indications that the absence may be adverse to national security interests.

1-4.2. U.S. Persons, Non-DoD-Affiliated Persons and Organizations, Non-DoD-Affiliated U.S. Citizens Outside the U.S.

a. Occasionally, elements of DoD have been subjected to criticism for investigative conduct that was perceived to be an infringement of basic privacy rights of U.S. citizens not affiliated with DoD and an unwarranted intrusion into the affairs of similarly non-affiliated U.S. organizations. In order to eliminate the basis for future criticism, DoD established guidelines (DoD Directive 5200.27) regarding the collection, retention, and dissemination of information on persons and organizations not affiliated with DoD within the U.S., and on non-DoD-affiliated U.S. citizens anywhere in the world. This directive is not applicable to the intelligence components of DoD and does not apply to criminal investigations. SECNAVINST 3820.2D applies these principles to DON and defines persons who are DoD-affiliated.

b. DoD Directive 5240.1 of April 25, 1988 provides authority and guidance to DoD intelligence components, to include the elements of NCIS conducting CI activities, to collect, retain, or disseminate information concerning U.S. persons for CI (vice criminal or security) purposes. CI collection must comply with DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons". SECNAVINST 3820.3E implements DoD Directive 5240.1 and DoD 5240.1-R.

1-4.3. Controversial Views. The First Amendment of the United States Constitution guarantees freedom of speech. Additionally, the Privacy Act (5 USC 552a) provides in section (e)(7) that, unless otherwise authorized, no agency shall maintain any records describing how an individual exercises First Amendment rights, including information concerning his or her religious and political beliefs or his opposition to official U.S. policy. Accordingly, the mere expression of controversial views, standing alone, cannot be considered a matter of official interest and will not be the basis for NCIS investigative action. Investigative action would only be appropriate under the following circumstances:

a. If the views expressed are coupled with the alleged commission of an act that in itself would be a violation of a statute, regulation, or directive. In this case, as in the following examples, the violation, not the expression of views, would form the basis for the investigation.

b. If the views are expressed in such a manner as to indicate the possibility of sedition. Under the UCMJ and other federal statutes, sedition involves acting in concert with another or others in opposition to lawful civil authority.

c. If the mode or manner of expression of views is in itself a violation of Article 88, UCMJ (contempt towards officials).

d. If the person is subject to the UCMJ and his/her communicated views are designed to promote disloyalty or disaffection of such nature as to constitute a violation of Article 134, UCMJ.

1-4.4. Dissident and Protest Activities. Closely allied with the above discussion as to controversial views are the DoD guidelines relating to dissident and protest activity by active duty members of the

Armed Forces. OPNAVINST 1620.1B implements DoD Directive 1325.6, which discusses authority and responsibility by the commander to prohibit certain on-base activity, such as unauthorized distribution of printed materials and demonstrations on base, and to define permissible and impermissible conduct of this nature by persons subject to the UCMJ. A violation of this regulation would be punished under Article 92, UCMJ. A detailed discussion of domestic security matters may be found elsewhere in NCIS-3.

1-5. INVESTIGATIVE MISSION

1-5.1. Criminal. The jurisdiction for NCIS to conduct criminal investigations purusant to SECNAVINST 5430.107, which defines the NCIS role in the more common types of criminal offenses. Depending on the circumstances, this jurisdiction may be shared with other agencies. Investigative jurisdiction refers to the propriety of NCIS conducting an investigation and is usually determined by the military interest in the case, regardless of the location of the crime. Local and federal laws controlling a particular area will determine whether state or federal civilian courts have jurisdiction over persons not subject to the UCMJ.

1-5.2. DOJ/DoD Memorandum of Understanding (MOU). In January 1985, a "Memorandum of Understanding Between the Department of Justice and the DoD Relating to the Investigation and Prosecution of Certain Crimes" was reissued. This MOU updates policy and procedures for criminal investigations conducted by the criminal investigative organizations of the DOJ and the DoD and is implemented by DoD Directive 5525.7.

1-5.3. Posse Comitatus Act. This act states in relevant part: "Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years or both" (18 USC 1385).

a. The Posse Comitatus Act, hereinafter referred to as the "Act," was originally enacted in 1878. Its purpose was to cure a perceived evil -- the indiscriminate use of federal troops to enforce the law. Prior to passage of the Act, troops were used for such things as: aiding revenue officers in suppressing illegal production of whiskey; assisting local officials in quelling labor disturbances; and insuring the sanctity of the electoral process in the South by posting guards at polling places. This proscription has evolved into a general prohibition against civil use of the military. Additionally, in 10 USC 375, Congress directed the Secretary of Defense to issue regulations that essentially apply the Act to the Navy and Marine Corps. Therefore, the principles of the Act have been adopted as federal policy throughout the DON by SECNAVINST 5820.7C (Cooperation with Civilian Law Enforcement Officials), which implements the DoD Directive 5525.5 on the same subject. Both regulations have provisions that exempt some civilian employees of DoD and DON from the limitations of the Posse Comitatus restriction, as long as he/she is not under the direct control of a military officer.

b. In January 1993, when our organization's name was changed from NIS to the NCIS, the position of the Director became a civilian billet, with direct reporting requirements and daily operational oversight residing in a strictly civilian chain of command. Currently, that chain of command is described in SECNAVINST 5430.107. The Director, NCIS reports directly to the

Secretary of the Navy. Headquarters NCIS is an Echelon 2 activity. Consistent with references (b) through (e) of the SECNAVINST 5430.107, the Under Secretary of the Navy, with the assistance of the General Counsel of the Navy, shall have responsibility for oversight of NCIS and shall serve as chair of the NCIS Board of Directors. In addition, the Director, NCIS serves as Special Assistant for Naval Investigative Matters and Security to the Chief of Naval Operations (CNO) (N09N). Thus, the NCIS organization from the civilian (1811) special agent in the field, through the Director and Under Secretary of the Navy, to the Secretary of the Navy, is entirely civilian. Additionally, NCIS' authority to initiate an investigation is independent of any military commander under DoD Instruction 5505.3. Thus, Posse Comitatus does not generally pose a problem for NCIS, with the exception of actions taken by military special agents, which is discussed in the following section.

c. The following policy is established:

(1) NCIS civilian special agents are not bound by the prohibitions of the Act.

(2) NCIS military special agents are bound by the prohibitions of the Act, however, the Act is not deemed to apply in those cases where there is a continuing, independent military or DoD interest to be served or protected. Although not intended to be all-inclusive or exclusive, the following are examples of a continuing independent interest, as set forth in SECNAVINST 5820.7C and DoD Directive 5525.5, (DoD Cooperation with Civilian Law Enforcement Officials):

(a) Actions related to the Commander's inherent authority to maintain law and order on a military installation or facility;

(b) Protection of classified military information or equipment;

(c) Protection of DoD personnel, DoD equipment, and official DoD guests; and

(d) Other actions undertaken primarily for a military or foreign affairs purpose.

1-5.4. Although investigative activity such as that described above is not prohibited by the Act, nothing in this section is to be construed as authorizing NCIS investigative action where it is otherwise prohibited or restricted by policy, regulation, or agreement. For example, the terms of the MOU referred to in Section 1-5.2. may operate to restrict investigative activity. SECNAVINST 5430.107 delineates the investigative jurisdiction of NCIS. Additionally, although investigative activity of the type and scope above is not prohibited by the Act, it is expected that the appropriate civilian authorities would be contacted in the early stages of an investigation and invited to participate in a joint investigative endeavor.

1-5.5. Other. The facilities of NCIS may be used by the DON where unusual circumstances or aspects of sensitivity attach that may require unusual techniques, and the exercise of a high degree of discretion, or the employment of extensive investigative resources. A prime example of the latter was the extensive use of NCIS special agents in connection with the debriefing of the members of the USS PUEBLO crew in 1969 following their release from North Korea.

a. Jurisdiction Over the Offense. With the exception of offenses triable by general court-martial under the laws of war, courts-martial have jurisdiction to try only offenses defined in the punitive articles of the UCMJ and those penal statutes incorporated within Article 134 under the Assimilative Crimes Act (18 USC 13).

b. Jurisdiction Over the Person. The jurisdiction of a court-martial depends solely on the accused's status as a person subject to the UCMJ.

c. Juvenile Delinquency. A juvenile who is alleged to have committed a violation of a law of the U.S. receives special consideration in the federal criminal justice system. However, the Federal Juvenile Delinquency Act has been held inapplicable to a service member for an offense punishable and tried under provisions of the UCMJ. When civilian juveniles are of investigative interest to NCIS, some familiarity with the applicable statutes is required.

(1) 18 USC 5031-42 addresses juvenile delinquency. The definition of a juvenile is contained in section 5031: "For the purpose of this chapter, a 'juvenile' is a person who has not attained his/her eighteenth birthday, or for the purpose of proceedings and disposition under this chapter for an alleged act of juvenile delinquency, a person who has not attained his twenty-first birthday, and 'juvenile delinquency' is the violation of a law of the United States committed by a person prior to his eighteenth birthday which would have been a crime if committed by an adult."

(2) 18 USC 5031 et. seq., concern arrest, detention, trial, and commitment, as well as the rights of juveniles. The intent of the law is to cause the proceedings to take place in the state court system, unless the state does not have available programs and services adequate for the needs of juveniles. Problems often arise in areas of exclusive Federal jurisdiction over which the state criminal courts (and juvenile courts) have no jurisdiction to prosecute.

(3) On occasion, NCIS special agents will need to take a juvenile into custody. Such cases should be immediately referred to appropriate civil authority. In exigent circumstances, a juvenile may be detained pending arrival of civil authorities. Although NCIS special agents will not generally be involved in custodial proceedings regarding juveniles, it is NCIS policy to comply with the general intent of Title 18, and, therefore, these guidelines are furnished for the handling of juvenile suspects:

(a) The suspect will be fully advised of his/her rights in language that he/she understands.

(b) Except in exigent circumstances, interrogation of a juvenile will not be undertaken, unless it has been coordinated with a parent, guardian, or custodian who has been advised of the rights of the juvenile and of the nature of the alleged offense, and who has been given a reasonable opportunity to be present. See also NCIS-1, Chapter 7 regarding the interrogation of juveniles.

(c) The Attorney General shall immediately be notified, by notifying the cognizant U.S. Attorney’s office.

d. Military Extraterritorial Jurisdiction Act (MEJA). MEJA (18 USC sections 3261-67) creates jurisdiction in U.S. Federal courts over civilians employed by or accompanying the Armed Forces

outside the U.S., certain service members, and former service members who engage in acts outside the U.S. that if done in the U.S. would be punishable by more than 1 year imprisonment. DoD Instruction 5525.11 implements this law in the DoD.

1-6. LAW ENFORCEMENT AUTHORITY

1-6.1. The commanding officer is responsible for providing full police and security functions for his/her unit. As found in Chapter 8, US Navy Regulations 1990: "The responsibility of the commanding officer for his command is absolute...." That responsibility cannot be delegated and no NCIS office is authorized to accept an attempted delegation of this responsibility. The barricaded captor/hostage situation is an example. In this type of situation, NCIS will provide advice and personnel to perform appropriate tasks, but the responsibility for the security of the command and all persons aboard remains with the commanding officer.

1-6.2. Authority to Apprehend and Arrest. A detailed discussion of the authority of NCIS special agents to apprehend and arrest, as well as the mechanics thereof, is contained in NCIS-3 Chapter 16.

1-6.3. Authority to Carry Weapons. The authority of NCIS special agents to carry firearms originates in Section 1585 of Title 10 USC, which provides: "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." Under this authority, the Secretary of Defense issued DoD Directive 5210.56, which further delegated this authority. This DoD Directive was implemented in the DON by SECNAVINST 5500.29C, which provides that the Director, NCIS, is delegated authority to arm appropriately trained NCIS personnel who are engaged in law enforcement, security and C duties. The Director may delegate this responsibility. NCIS-1, Chapter 34 addresses authority to carry weapons.

1-6.4. Authority to Administer Oaths. All NCIS special agents, civilian and military, have the authority to administer oaths and to take sworn statements in connection with their official investigative duties. This authority is identified in SECNAVINST 5430.107 and is derived from Article 136(b)(4), UCMJ, in the case of military special agents and from 5 USC 303, for civilian special agents. In fact, any employee of the DoD lawfully assigned to investigative duties may administer oaths to witnesses in connection with an official investigation.

1-6.5. Protective Operations. Recent years have seen a proliferation in the nature and scope of protective services provided by NCIS. In response to this additional tasking, NCIS provides specialized training to special agent personnel. NCIS-1, Chapter 35 is devoted to the technical aspects associated with protective service assignments.

a. SECNAVINST 5430.107, assigns NCIS as the executive agent for all protective service matters within the DON. NCIS has exclusive jurisdiction and authority to conduct and coordinate protective service operations to protect individuals who occupy designated DON High Risk Billets and other designated individuals, except as authorized by a combatant commander in a joint area of operations.

b. The U.S. Secret Service has protective responsibility for the President of the United States and other persons as described in 18 USC 3056. The following instructions govern this relationship: DoD Directive 3025.13, "Employment of DoD Resources in Support of the United States Secret Service," DoD Instruction 5030.34, "Agreement Between the United States Secret Service and the DoD Concerning Protection of the President and other Officials."

1-7. THREAT WARNING AND ANALYSIS

Multiple Threat Alert Center (MTAC). NCIS maintains, directs, and operates the DON MTAC to provide indications and warning of terrorist, foreign intelligence, cyber, and criminal threats to the DON and to generate related analysis and production on matters of interest to the Department. The MTAC serves as the NCIS fusion center for law enforcement, intelligence, CI, security, and other threat information required to defeat terrorist, foreign intelligence, criminal, and related threats to DON personnel, installations, facilities, vessels, and aircraft, and it supports the national effort to combat terrorism. In addition, the MTAC serves as the NCIS operational control center, providing direct support to NCIS investigations and operations as required.

CHAPTER 2
TITLE: FUGITIVE CASES
POC: CODE 23A
DATE: JUL 08

2-1. DISCUSSION

2-1.1. General

This category of offense is to be used when NCIS becomes involved in a fugitive investigation. The fugitive may be military or civilian, and the case may be state, local, federal, or solely an NCIS related matter. The status of the fugitive and circumstances surrounding the initiation of the investigation must be thoroughly understood in order to properly conduct the case. Fugitive investigations demand creativity, patience, and persistence for successful resolution. The case category for Fugitive investigations is 7F.

2-1.2. Definitions

a. Fugitive. A person who flees a jurisdiction to avoid prosecution for a crime or giving testimony in any criminal proceeding.

b. Unauthorized Absence (UA)/Absence Without Leave (AWOL). A member of the armed forces who, without authority, fails to go to his or her place of duty at the time prescribed; departs from that place; or absents himself or herself from his/her unit, organization, or place of duty at which the member is required to be at the time prescribed.

c. Desertion. A member of the armed forces who, without authority, goes or remains absent from his/her unit, organization, or place of duty with the intent to permanently remain away.

d. Missing Persons Investigation. Investigation of the unexplained disappearance of an individual where foul play, unusual or suspicious circumstances are alleged.

2-1.3. Criminal Law/Jurisdiction.

a. Uniform Code of Military Justice (UCMJ). Along with consideration for attempts and conspiracies. An individual who becomes a fugitive may have been charged or suspected of committing other criminal offenses as enumerated in the UCMJ. Crimes of this category are potentially violations of the UCMJ:

(1) Article 85 (Desertion)

(2) Article 86 (Absence Without Leave)

b. Federal Laws/United States Code (USC). An individual who becomes a fugitive may have been charged or suspected of committing a criminal offense as listed in United States Code. Fugitives are specifically discussed under Title 18 USC Sections 1071 through 1074 (Fugitives From Justice).

c. State Criminal Law. States will have specific laws governing fugitives and extradition agreements.

2-2. POLICY AND GUIDANCE

2-2.1. NCIS Authority

SECNAVINST 5430.107 (28DEC05), "Mission and Functions of the Naval Criminal Investigative Service," develops NCIS authority and jurisdiction to investigate this category of offense and gives NCIS jurisdiction over fugitive investigations due to possible underlying major criminal offenses the fugitive might be fleeing. Absent some urgent or unique circumstance that would indicate that a Fugitive (7F) investigation is warranted, command assets should handle uniquely military offenses under the UCMJ, such as desertion and UA. DoD Directive 5525.7, "Implementation of the Memorandum of Understanding (MOU) Between the Departments of Justice (DOJ) and Defense Relating to the Investigation and Prosecution of Certain Crimes," implements the MOU between DOJ and the DoD criminal investigative organizations, providing policy and guidance for criminal investigations when both departments have jurisdiction. An MOU exists between the United States Marshals Service (USMS) and NCIS, "USMS and NCIS MOU Regarding The Apprehension of Violent Fugitives" (18SEP96), which states that NCIS and the USMS "combine resources for the apprehension of Navy deserters wanted for underlying crimes of violence and major drug offenses." This MOU outlines the specific process for coordinating between NCIS and the USMS. Appendix (3) is a copy of the MOU with USMS.

2-2.2. NCIS Responsibility

When a suspect of a NCIS related investigation becomes a fugitive or an escapee from a Naval Correctional Facility, a 7F investigation will be initiated. The 7F Report of Investigation (ROI) (OPEN) will reference the original-offense investigation and remain open as long as the fugitive is at large.

2-2.3 All 7F investigations will be initiated as Special Interest (SI) investigations. NCIS-1 Chapter 45, "Managing Investigations" and NCIS-1 Chapter 25, "Report Writing," provide

policy for the initiation of SI investigations. An email address of "SI – Special Interest" is listed in the NCIS legacy email account for email correspondence to NCISHQ Code 23B DSI/SI desk officer. The ROI(OPEN) and/or subsequent ROI(INTERIM) reporting will be sent via information copy to the NCISHQ Code 23B DSI/SI desk officer (fugitive investigations).

2-2.4. A 7F investigation will be initiated upon request for assistance regarding a fugitive from state, local, or federal law enforcement or prosecuting agency.

2-2.5. ROI (OPEN) and all subsequent reporting will include an information copy to the Counterintelligence Directorate, NCISHQ Code 22, on those investigations of a National Security or counterintelligence interest (i.e. UCMJ Articles 92,106, and 106a) and all fugitive cases where the subject has a security clearance. The Combating Terrorism Directorate, NCISHQ Code 21, will be notified for investigations relating to Counterterrorism matters.

2-2.6. The apprehension of the fugitive is to be effected according to the guidance contained in NCIS-3 Chapter 16, "Arrest Authority and Military Apprehension."

2-2.7. Once the fugitive is apprehended, immediate contact must be made with the fugitive's command to coordinate his/her return to military authority. Commands should be advised to solicit assistance from the appropriate Deserter Information Point and Navy Absentee Collection Unit and Information Center (NACIC), Great Lakes, IL, or the Marine Corps Absentee Collection Center (MCACC), Headquarters, USMC, Washington, DC. Special agents are recommended to consult with the NACIC or MCACC to coordinate investigative efforts upon determination that a military subject is a fugitive.

a. For more information regarding the NACIC, such as contact numbers and locations, see their website at http://www.npc.navy.mil/CommandSupport/CorrectionsandPrograms/NACIC+Home.htm.

b. For more information regarding the MCACC, such as contact numbers and locations, see their website at http://hqinet001.hqmc.usmc.mil/pp&o/PS/psl/corrections/absenteeCollection.asp.

2-2.8. As a matter of routine, NCIS does not become involved with the transportation of fugitives. If circumstances dictate that NCIS special agents transport a fugitive, the Fugitive Investigations Desk Officer (DSI/SI Desk Officer), NCISHQ Code 23B, must be contacted and SAC/NCISHQ approval/concurrence obtained. Prior to utilizing NCIS special agents for a prisoner transport mission, consideration should be given to determining the availability of the USMS Prisoner Transportation System.

2-2.9. Missing Persons. In situations where an individual has disappeared under unexplained circumstances and foul play, unusual or suspicious incidents are alleged then the investigating agent should consider opening a Missing Persons investigation (7M). Missing Persons investigations differ from Fugitive investigations in that the missing person may be the victim of a crime and a fugitive is a suspect in a crime who is fleeing justice. See NCIS-3, Chapter 42 (Missing Persons) for further discussion.

2-2.10. DD Form 553, “Deserter/Absentee-Wanted by the Armed Forces”

The DD Form 553 is the only recognized means by which civilian law enforcement can apprehend members wanted for UCMJ offenses. If the fugitive is an active duty military member, the member's command promptly issues a DD Form 553. Upon the command issuing the DD Form 553, discussion should be initiated as to the member's disposition following his/her return. DoD Directive 1325.2, “Desertion and Unauthorized Absence,” provides further details regarding desertion and UA. Special agents should consult with the NACIC or the MCACC, as appropriate, in regard to military members who become fugitives. Appendix (1) is the DD Form 553.

2-2.11. Media Affairs

The responsible use of the news media as an aid in a 7F investigation should not be overlooked and is recommended as a valuable option. NCIS-1, Chapter 42 “Public Affairs”, provides guidance relating to policy and technical aspects of the release of information by NCIS to the media. The news media can play a significant role in resolving a fugitive case by providing investigators with a timely means of distributing information over a broad geographic region. The timing, appropriateness, and style of a news release can be critical to the results of an investigation and should be evaluated early in the case.

2-2.12. Coordinate electronic and print media use with the local Navy public affairs officer and/or the local police public affairs staff if the investigation is concurrent. If an investigation requires media support from a national level news service to solicit information on a local fugitive investigation, coordination with the NCISHQ Code 00C, Communication Directorate should be initiated.

2-3. ELEMENTS OF THE CRIME

2-3.1. Fugitive Cases

a. In many situations, a suspect has become a fugitive after the allegation or completion of adjudicative actions for a particular offense that is not related to being a fugitive. The two purely military offenses that result in the accused becoming a fugitive are Article 85, “Desertion,” and Article 86, “Absence without Leave,” of the UCMJ.

b. For civilian fugitives, application of federal, state, and/or local statutes would be determined after consultation with the appropriate law enforcement and prosecuting agency.

2-3.2. Essential Elements of Desertion

Any member of the armed forces who:

a. Leaves or remains absent without authority from unit, organization, or place of duty with intent to remain away permanently;

b. Quits unit, organization, or place of duty with intent to avoid hazardous duty or shirk important service; or

c. Enlists or accepts an appointment in one of the armed forces without fully disclosing the fact that he/she has not been regularly separated from the same or other armed forces division; or

d. Enters any foreign armed service, except when authorized by the United States; is guilty of desertion.

e. Any commissioned officer of the armed forces who, after tender of his/her resignation and before notice of its acceptance, quits his/her post or proper duties without leave and with the intent to remain away permanently is guilty of desertion.

2-3.3. Legal Discussion – Desertion

a. Under Article 85 of the UCMJ, there are four types of desertion:

(1) Desertion with Intent to Remain Away Permanently;

(2) Desertion with Intent to Avoid Hazardous Duty or to Shirk Important Service;

(3) Desertion Before Notice of Acceptance of Resignation; and

(4) Attempted Desertion.

b. The intent to remain away permanently may be formed at any time during the UA. The intent need not exist throughout the absence, or for any particular period of time, as long as it exists at some time during the absence. The intent to remain away permanently may be established by circumstantial evidence.

2-3.4. Legal Discussion – AWOL

a. This offense is referred to as "UA" in the United States Navy and United States Marine Corps and "AWOL" in the United States Army and United States Air Force. Any member of the armed forces who, without authority, fails to go to appointed place of duty at the time prescribed, departs from that place, or absents himself/herself from the unit, organization, or place of duty at which the member is required to be at the time prescribed, shall be AWOL.

b. Article 86 is designed to cover every case not elsewhere provided for where it is the armed forces member's own fault that he/she is not in the required place at the prescribed time.

c. The allegations of failing to go to or leaving the appointed place of duty require proof that the accused actually knew of the appointed time and place of duty. Actual knowledge may be proved circumstantially. Specific intent is not an element of UA.

2-4. INVESTIGATIVE PROCEDURE

2-4.1. Considerations

The following sections are suggestions for any investigating agent to keep in mind when involved in a fugitive investigation. The fugitive investigation (7F) is differentiated from a missing person investigation (7M) in that a fugitive is a person who unlawfully flees to elude arrest or prosecution, while a missing person involves a situation where the individual has gone missing for unexplained reasons or where the missing person is the victim of a crime. In either case (Fugitive or Missing Persons) the case agent should consult/notify the NCISHQ Code 23B DSI/SI desk officer regarding the initiation of an investigation.

2-4.2. Headquarters Support

At the field office level, appropriate database checks such as Auto Track, Department of Defense Employee Interactive Data System (DEIDS), Law Enforcement Information Exchange (LInX), National Crime Information Center (NCIC), National Law Enforcement Telecommunications System (NLETS), Defense Central Index of Investigations (DCII), El Paso Intelligence Center (EPIC), and other databases will be conducted. The Multiple Threat Alert Center Law Enforcement (MTACLE) unit is a 24/7 resource intended to augment local system capabilities; however, it is not intended to replace local routine database queries. The MTACLE unit should be contacted after normal working hours or whenever field personnel are operational, conducting surveillance, or cannot otherwise gain access to databases to conduct checks locally. The MTACLE unit can be contacted by E-mail (b)(6), (b)(7)(C) ncis.navy.mil) or telephone(b)(6), (b)(7)(C) (b)(6), (b)(7)(C) in support of fugitive investigation database queries.

2-4.3. NCISHQ Code 23B DSI/SI desk officer (fugitive investigations) can also liaison with the NACIC, the MCACC, the United States Marshals Service, and Interpol.

2-4.4. Requests for investigative assistance from NCIS Contingency Response Field Office (CRFO). The investigating office of a fugitive investigation may request investigative assistance from the CRFO. Requests and coordination should be done via the pertinent field office management, the CRFO senior management, and NCISHQ Code 23B. The decision to receive CRFO support will rest with NCISHQ Code 23B and CRFO senior management, based upon such things as the difficulty of investigation, urgency of the investigation, how funding will be provided, etc. If support is to be provided, the case agent will send an ROI(ACTION) to CRFO making the formal request and detailing what assistance is being requested from CRFO. CRFO will provide an ROI(ACTION) return indicating their level of support to the requesting office. Both ROI(ACTION) will be info copied to NCISHQ Code 23B.

2-4.5. Delivery of Fugitive Members, Civilians, and Dependents to State, Federal, and Foreign Authorities

Coordination with the appropriate judge advocate is highly recommended prior to the serving of any fugitive warrant to avoid problems, delays and determine if any circumstances exist where delivery can be refused for members under Section 0610, “Circumstances for Refusal of Delivery,” of the Judge Advocate General (JAG) Manual.

2-4.6. Delivery When Persons are Within Territorial Limits of the Requesting State

a. When the delivery of any fugitive member or civilian is requested by local civil authorities of a state (includes the District of Columbia, territories, commonwealths, and all possessions or protectorates of the United States) for an offense punishable under the laws of that jurisdiction and he/she is located at a Naval or Marine Corps installation within the requesting jurisdiction or aboard a ship within the territorial waters of such jurisdiction, commanding officers are authorized to and normally will deliver such person when a proper fugitive warrant is issued. For military members, delivery to state authorities will only be effected upon compliance with Section 0607, "Delivery of Agreement," of the JAG Manual and completion of a written agreement that conforms to Appendix A-6-b of the JAG Manual.

b. Dependents, civilian employees, and civilian contractors and their employees fall under the guidance in Section (a) except Section 0607 and Section 0610 of the JAG Manual do not apply.

2-4.7. Delivery When Persons are Beyond Territorial Limits of the Requesting State

a. After consulting with a Naval or Marine Corps judge advocate and upon compliance with Section 0607 and subject to the exceptions in Section 0610 of the JAG Manual, any officer exercising general court-martial jurisdiction (or officer designated by the exercising officer) or any commanding officer is authorized to deliver a member to state authorities upon presentation of a fugitive warrant.

(1) If the member voluntarily waives extradition, a witnessed written statement must be drafted to include that the member signing it has received counsel of either a military or civilian attorney prior to executing the waiver and the name and address of the attorney consulted. The waiver should be substantially as that in Appendix A-6-a of the JAG Manual.

(2) If refusing to waive extradition, the member will have the opportunity to contest extradition in the courts of the state in which the member is located.

b. The requirements of sections 0607 and 0610 of the JAGMAN apply to active duty personnel only. After consulting with a Navy or Marine corps Judge advocate, a commanding officer is authorized to deliver dependents, civilian employees, and civilian contractors and their employees located on a Department of the Navy (DON) installation to state authorities upon presentation of a fugitive warrant.

2-4.8. Federal Authorities. When federal law enforcement authorities display proper credentials and federal arrest warrants for the arrest of members, civilian employees, civilian contractors and their employees, or dependents residing at or located on a DON installation, commanding officers are authorized and should allow the arrest of the individual sought. Section 0607 of the JAG Manual is not a condition of delivery of members, but Section 0610 of the JAG Manual may be applied to members.

2-4.9. Persons Stationed Outside the United States

a. It is the policy of the DON to cooperate with Federal, state and local courts in enforcing court orders. The DON will cooperate with requests when such action is consistent with mission requirements, the provisions of international agreements and ongoing DoD investigations and courts-martial. See DoD Instruction 5525.09 (10FEB06), "Compliance of DoD Members, Employees, and Family Members Outside the United States with Court Orders," which is implemented in SECNAVINST 5820.9A (04JAN06), “Compliance with Court Orders by Department of the Navy Members, Employees, and Family Members outside the United States.”

b. Court ordered requests to return DON military members to the United States for felonies will normally be granted and can be ordered by appropriate DON authority. The Federal District court requesting delivery of any member of the Navy or Marine Corps, upon appropriate representation by the DOJ to the Secretary of the Navy (JAG), will have the member returned to the United States at the expense of the DON and held at a military facility convenient to the DON and the DOJ.

c. Court ordered requests for the involuntary return DON civilian employees to the United States for felonies cannot be forced by DON officials. DON employees will be strongly urged to comply with court orders. However, failure by the employee to comply with court orders involving felonies will normally require processing for adverse action, up to and including removal from Federal service.

d. Court ordered requests for the involuntary return DON military dependents to the United States for felonies cannot be forced by DON officials. DON military dependents will be strongly urged to comply with court orders. However, failure by the military dependent to comply with court orders involving felonies will normally have their command sponsorship removed.

e. Under the Military Extraterritorial Jurisdiction Act of 2000 (MEJA) United States contractors and United States civilian employees overseas and employed by the armed forces, can be subject to prosecution in United States Federal Courts for any offense at the felony level. Jurisdiction of federal statutes extends to United States nationals within the special maritime and territorial jurisdiction of the United States.

2-4.10. Delivery of DON Persons to Foreign Authorities. Except when provided by agreement between the United States and the foreign government concerned, commanding officers are not authorized to deliver DON members or civilian employees or their dependents residing at or located on a Navy or Marine Corps installation to foreign authorities. When a request for delivery of these persons is received in a country with which the United States has no agreement, contact is to be made with the appropriate judge advocate. In either situation the United States embassy in the country in question should be informed and coordinated with regarding any requests of a foreign government for the turn over of a DON member or civilian employee. Status of forces agreement guidance is contained in DoD Directive 5525.1, “Status of Forces Policies and Information,” and SECNAVINST 5820.4G, “Status of Forces Policies, Procedures, and Information.”

2-4.11. Procedure

The following sections relate to the procedural aspects of a fugitive investigation.

a. DoD Directive 1325.2 (02AUG04), "Desertion and Unauthorized Absence." A deserter involved in one or more of the aggravating offenses listed in Appendix (2) of this chapter are considered aggravated circumstances in those cases of desertion.

(1) Block 19 of the DD Form 553 must include all of the aggravated offenses (Appendix (2)) the fugitive is suspected of as well as any safety advisements such as armed and dangerous, escape risk, etc. Once the required DD Form 553 is issued, the field will make an NCIC Wanted Person entry, via SPINTCOM (b)(6), (b)(7)(C) or email at (b)(6), (b)(7)(C)@navy.mil.). If the fugitive presents a danger to himself/herself or others, SPINTCOM can be requested to add a special message key to indicate "caution" to the original entry (see the NCIC Manual for additional guidance).

b. Notifications. The NCIS special agent will obtain a full description of the fugitive and obtain a recent photograph. Photographs can be obtained from a state driver's license, Common Access Card (CAC), facility access cards, cruise books, school year books/graduation photograph, command photographs, mug shot/police reports, etc. The NCISHQ Code 23B DSI/SI desk officer (fugitive investigations) should be contacted to coordinate the completion of the NCIS public website entry (NCIS Most Wanted), a fugitive wanted poster, and initiation of the fugitive investigation. An ROI(ACTION) lead should be sent to NCISHQ Code 23B DSI/SI desk officer for the approval and submission of the wanted poster and subject information. For expeditious posting, the information and image may be emailed to the DSI/SI desk officer, to be followed by an ROI(ACTION). All subsequent ROI(INTERIM) reporting in the fugitive investigation should have information copies forwarded to NCISHQ Code 23B DSI/SI desk officer (fugitive investigations).

The "NCIS Most Wanted Fugitives" website is maintained by the Communications Directorate, NCISHQ Code 00C. The "Wanted Fugitive Poster" can be downloaded from the NCISnet (in the "Forms" portion of the "Downloads" section: https://infoweb.ncis.navy.mil/downloads-forms.html), filled out by the case agent, and forwarded to the NCISHQ Code 23B DSI/SI desk officer (fugitive investigations) for submission to NCISHQ Code 00C. Photographs of suspects are to be formatted in JPEG and attached to email for insertion into the poster. The following should also be considered in a fugitive investigation:

(1) For military members who are listed as deserters, but have not committed any other offenses, an appropriate NLETS message, via SPINTCOM, will be sent to the local law enforcement agencies in the deserter's hometown, place of residence, and involved geographical region. This is generally done by the member's command or other military authority. For military members, it is recommended to contact the NACIC or the MCACC to coordinate possible investigative leads.

(2) For civilian fugitives and military members who are fugitives as a result of criminal activity, NCIS field elements will make entries into NCIC/NLETS, via SPINTCOM. This will

be done by sending an ROI(ACTION) to NCISHQ Code 15C2 with the information provided in the NCIC wanted person format. For expedited action send to SPINTCOM via phone at (b)(6), (b)(7)(C) (b)(6), (b)(7)(C) or email at (b)(6), (b)(7)(C) @navy.mil, but should also be followed up by an ROI(ACTION). The NCIC-2000 "Wanted Person File Entry" form can be found on the NCISNet (in the "Forms" portion of the "Downloads" section: https://infoweb.ncis.navy.mil/downloads-forms.html). Once the suspect has been apprehended, the originating office must send another ROI(ACTION) to NCISHQ Code 15C2 using the NCIC wanted persons form to clear the entry in NCIC. In a joint investigation involving a civilian fugitive, NCIS will coordinate NCIC/NLETS entries with the participating agency to avoid duplication.

(b)(7)(E)

(5) Conduct a review of personnel and medical records.

(6) Obtain and enter a legible copy of the fugitive's fingerprints and dental records into evidence for possible future identification. If necessary, consult the senior local Dental Corps representative and using the NCIC Code Manual Personal Descriptors Dental Information section, have the person's dental record coded for NCIC entry in coordination with the SPINTCOM (NCISHQ Code 15C2).

(7) Interview command personnel, neighbors, parents, and other relatives as well as personal friends for possible leads, interviewing persons known to have seen the fugitive last in more detail.

(8) Conduct a check of local jails, morgues, hospitals, and psychiatric institutions under the person's real name, aliases, and Jane/John Doe.

(b)(7)(E)

(12) For long term cases, check with city/county records such as tax assessor, voter registration, county recorder, Social Security Administration, Department of Labor (state and Federal) and Internal Revenue Service.

(13) If after a period of time no leads have surfaced, consider revisiting some of the above leads.

(14) When investigative leads indicate a suspect may have fled the United States to another country, the field elements will immediately contact the NCISHQ Code 23B DSI/SI desk officer (fugitive investigations), who will assist in contacting the following agencies. The use of these agencies services will be utilized simultaneously.

(a) International Criminal Police Organization (INTERPOL). A RED NOTICE can be pursued via INTERPOL to notify the international community that a suspect is being sought. The case agent will coordinate with NCISHQ Code 23B DSI/SI desk officer (fugitive investigations) to obtain the RED NOTICE form from INTERPOL, and complete it with the assistance of the NCISHQ DSI/SI desk officer and submit it to INTERPOL via NCISHQ. It is important to note two requirements must be met before a RED NOTICE can be published. First, a Form DD-553 for military deserters must be obtained. Second, a commitment to extradite the suspect must be made by the prosecutor or military command.

(b) USMS. The USMS is the primary federal law enforcement agency responsible for bringing persons who have violated federal criminal law to the United States from foreign countries. USMS also has the responsibility of performing all federal and state extraditions to the United States and can be contacted through local fugitive task forces set up in all federal court districts. USMS can often assist in locating fugitives in foreign countries and assist, through an MOU, in transferring the fugitive back to the United States when appropriate. Case agents should maintain communications with the NCISHQ Code 23B DSI/SI desk officer (fugitive investigations) regarding USMS coordination and can request NCIS assistance in making contact if no regional task force exists.

(c) Department of State (DOS). DOS Diplomatic Security Service (DSS) maintains a presence in most countries as Regional Security Officers and can provide assistance in locating and apprehending United States fugitives. A request for DSS services should originate with the NCISHQ Code 23B DSI/SI desk officer (fugitive investigations) with input from the case agent.

2-4.12. Fugitive Review Board – Investigation Longevity. Fugitive investigations will be either civilian or military members who are fleeing legal actions or in fear of legal action. Once a suspect has been determined to be a fugitive and a fugitive investigation is initiated, the investigation cannot be closed for lack of investigative leads, inability to determine the suspect's location, or that the suspect has fled to a foreign country. This may result in an investigation that languishes or is difficult to maintain in an "open" status. Therefore, the NCISHQ Code 23B Fugitive Review Board (FRB) has been established to examine fugitive investigations in order to further the investigation. As stated in previous sections of this chapter, the NCISHQ Code 23B DSI/SI desk officer (fugitive investigations) will be consulted at the initiation of a fugitive investigation; however, the FRB is to be utilized when all logical leads have been exhausted and

the subject remains unlocated or the subject has fled from U.S. jurisdiction (i.e. a foreign country).

a. Requesting an NCISHQ FRB. When a field office has determined that a fugitive investigation should no longer remain in an active status, the case agent will send an ROI(ACTION) lead to the NCISHQ Code 23B DSI/SI desk officer (fugitive investigations) to request an FRB. The FRB will be convened to examine the fugitive investigation and determine if any additional investigative steps should be taken. The FRB will make those instructions to the case agent, or the FRB will direct the pertinent fugitive investigation be placed in an "inactive" status.

(1) Additional Investigative Steps. If the FRB directs further steps, an ROI(ACTION) will be sent to the originating office from NCISHQ Code 23B delineating those instructions to the case agent for action. The investigation will remain in an "open" status, requiring the continuation of the 60 day reporting requirement. Upon completion of directed actions, the case agent should once again request an FRB, using the same process.

(2) "Inactive" Status. If the FRB determines that the investigation has exhausted all logical investigative leads and the suspect is still unlocated or the suspect has fled U.S. jurisdiction, the FRB will send an ROI(ACTION) back to the originating office recommending the pertinent fugitive investigation to be placed in an "inactive" status. This status does not infer that the investigation is closed; however, it allows the case agent to suspend the 60 day reporting requirement. Instead the case agent will be required, on an annual basis, to file an ROI(INTERIM) describing any changes, updates, or pertinent information. If at any point after the investigation goes to "inactive" new information is developed or the suspect is located, the case will revert to an "open" status, which includes the return to 60 day reporting. The case agent can once again request an FRB if the investigation does not come to a resolution. The annual reporting should include any new developments and investigative attempts such as: database checks (e.g. NCIC); contact with family and/or friends of suspect; and contact with local police department of logical location(s) of interest.

(3) Fugitive investigations can only be closed upon apprehension or change in legal status of the suspect. Closure of a fugitive case does not require FRB approval.

b. The NCISHQ Code 23 FRB will consist of the following voting members:

(1) Code 23B Division Chief, Criminal Investigations;

(2) Code 23B Desk Officer, Crimes Against Persons;

(3) Code 23A Program Manager, General Crimes; and

(4) Other member(s) as necessary or appropriate.

APPENDIX (1)

DD Form 553 - DESERTER/ABSENTEE-WANTED BY THE ARMED FORCES

DESERTER/ABSENTEE WANTED BY THE ARMED FORCES

1. DATE PREPARED *(YYYYMMDD)*

REPORT CONTROL SYMBOL: DD-P&R(SA)1454

2. TO *(Local, State or Federal law enforcement authority as indicated by Military Deserter Information Point)*

3. FROM *(Organization or activity and place from which absent. If unauthorized absence occurs in transit, list old and new unit in Remarks)*

4. DISTRIBUTION

5. ABSENTEE IDENTIFICATION

a. NAME *(Last, First, Middle Initial)*

b. GRADE/RANK/RATE

c. SEX

d. RACE *(X one or more)*

- [ ] AMERICAN INDIAN/ALASKA NATIVE
- [ ] ASIAN
- [ ] BLACK OR AFRICAN AMERICAN
- [ ] NATIVE HAWAIIAN OR OTHER PACIFIC ISLANDER
- [ ] WHITE
- [ ] DECLINE TO RESPOND

e. ETHNICITY *(X one)*

- [ ] HISPANIC OR LATINO
- [ ] NOT HISPANIC OR LATINO
- [ ] DECLINE TO RESPOND

f. PLACE OF BIRTH *(City, State, Country)*

g. DATE OF BIRTH *(YYYYMMDD)*

h. HEIGHT

i. WEIGHT

j. EYE COLOR *(X one)*

- [ ] BLACK
- [ ] BLUE
- [ ] BROWN
- [ ] GREEN
- [ ] GRAY
- [ ] HAZEL
- [ ] VIOLET

k. HAIR COLOR *(X one)*

- [ ] AUBURN
- [ ] BLACK
- [ ] BLOND
- [ ] BROWN
- [ ] GRAY
- [ ] RED
- [ ] SILVER
- [ ] WHITE
- [ ] BALD

l. DIP CONTROL NUMBER

m. BRANCH OF SERVICE

n. SOCIAL SECURITY NO.

o. CITIZENSHIP

p. MARITAL STATUS

q. MILITARY OCCUPATION

r. CIVILIAN OCCUPATION

s. PERMANENT RESIDENCE ADDRESS *(Include ZIP Code)*

6. CURRENT ENLISTMENT

a. DATE *(YYYYMMDD)*

b. PLACE *(City and State)*

7. ENTRY INTO CURRENT PERIOD OF SERVICE

a. DATE *(YYYYMMDD)*

b. PLACE *(City and State)*

8. ATTACH PHOTOGRAPH *(If available)*

9. TIME OF ABSENCE

a. DATE *(YYYYMMDD)*

b. HOUR

10. ADMINISTRATIVE DATE OF DESERTION *(YYYYMMDD)*

11. ESCAPED OR SENTENCED PRISONER *(X as applicable)*

- [ ] YES
- [ ] NO

IF "YES," SPECIFY CHARGE

12. DISCHARGE STATUS *(X as applicable)*

a. DISCHARGED [ ] YES [ ] NO

b. SUSPENDED [ ] YES [ ] NO

13. OPERATOR'S LICENSE

a. NUMBER

b. STATE

c. EXP. DATE *(YYYYMMDD)*

14. VEHICLE LICENSE

a. PLATE NO.

b. STATE

c. EXP. DATE *(YYYYMMDD)*

d. TYPE

15. VEHICLE

a. VEHICLE IDENTIFICATION NUMBER

b. YEAR

c. MAKE

d. MODEL

e. STYLE

f. COLOR

16. RELATIVES AND/OR PERSONS KNOWN BY ABSENTEE *(If more space is needed, continue in Remarks or on a separate page, making reference to this item number.)*

a. NAME *(Last, First, Middle Initial)*	b. ADDRESS *(Include ZIP Code)*
(1)	
(2)	
(3)	
(4)	
(5)	

DD FORM 553, MAY 2004 PREVIOUS EDITION IS OBSOLETE. Page 1 of 3 Pages

Reset

17. CERTIFICATION *(See Notes)*

The undersigned states: That he/she is a commissioned officer of the United States _____ *(Military Department),* presently assigned as the Commanding Officer, _____ *(Unit from which the alleged deserter absented himself or herself),* and in the performance of official duties imposed by Department of Defense Directive 1325.2 and _____ *(Regulations of the Service concerned which implement DOD Directive 1325.2, e.g. Army Regulations 190-9 and 630-10),* he/she has conducted an investigation into the status of _____ *(Name and rank of alleged deserter),* a member of the United States Armed Forces serving on active duty with _____ *(Unit and Service from which the alleged deserter absented himself or herself),* by questioning his/her unit cohorts; by examining and verifying the field service records of said service member which reflect his/her duty status; by requesting the member's next of kin to urge his/her voluntary return to military control if they are aware of his/her whereabouts; by inquiring to the fullest extent possible into the feasibility of other explanations for the member's absence, to include sickness, injury, hospitalization, and confinement by civil law enforcement officials; and officially ordered diversion from his/her unit of assignment by querying the member's losing unit (and en route temporary duty unit), the appropriate career management division, the servicing replacement organization, and the servicing Military Personnel and Transportation Assistance Office (and *(See Note 1)* _____). That based on the aforesaid investigation, the undersigned has personal knowledge that, on or about _____ *(Date - YYYYMMDD),* _____ *(Name and rank of alleged deserter),* did, without authority and with intent to remain away therefrom permanently, absent himself/herself from his/her unit/organization/place of duty, to wit: *(See item 3 above)* located at *(See item 3)* in violation of Section 885, Title 10, United States Code and he/she has remained continuously so absent until _____ *(Date this statement is executed - YYYYMMDD).* I state under penalty of perjury (under the laws of the United States of America *(See Note 2)* that the foregoing is true and correct. Executed on _____ *(Date - YYYYMMDD).*

NOTES:

1. For use only when a servicemember fails to report to a gaining unit of assignment during a permanent change of station.
2. For use only when statement is executed outside the United States, its territories, possessions and commonwealths.

18. COMMANDING OFFICER

a. TYPED NAME *(Last, First, Middle Initial)*	b. RANK	c. TITLE	
d. ORGANIZATION AND INSTALLATION	e. SIGNATURE *(All copies)*		f. DATE SIGNED *(YYYYMMDD)*

19. REMARKS *(List peculiar habits and traits of character; unusual mannerisms and speech; peculiarities in appearance; clothing worn; aliases (names); marks and scars; tattoos; facial characteristics; complexion, posture; build, other SSN's used by individual; or other data that may assist in identification.*

INFORMATION

1. AUTHORITY TO APPREHEND.

a. Any civil officer having the authority to apprehend offenders under the laws of the United States, or of a State, territory, commonwealth, possession, or the District of Columbia may summarily apprehend deserters from the Armed Forces of the United States and deliver them into custody of military officials. Receipt of this form and a corresponding entry in the FBI's NCIC Wanted Person File, or oral notification from military officials or Federal law enforcement officials that the person has been declared a deserter and that his/her return to military control is desired, is authority for apprehension.

b. Civil authorities may apprehend absentees (AWOL's) when requested to do so by military authorities.

2. PAYMENT OF REWARD OR REIMBURSEMENT FOR EXPENSES.

a. Rewards. Receipt of this form, or oral or written notification from military authorities or Federal law enforcement officials, prior to apprehension of the individual, that the person is an absentee and that his/her return to military control is desired will be considered as an offer of reward. Persons or agency representatives (except salaried officers or employees of the Federal Government or servicemembers) apprehending or delivering absentees to military control are authorized:

(1) Payment for apprehension and detention of absentees until military authorities assume custody; or

(2) Payment for apprehension and delivery of absentees to a military installation.

b. Reimbursement for Expenses. Reimbursement may be made for actual expenses incurred when conditions for payment of a reward cannot be met. If two or more persons perform these services, payment will be made jointly or severally, but total payment to all may not exceed prescribed limitations.

c. Payment. Payment will be made to the person or agency representative actually making arrest and detention or delivery by the disbursing officer servicing the military facility to which the absentee is delivered and will be in full satisfaction of all expenses of apprehending, keeping and delivering the absentee. Payment may be made whether the absentee surrenders or is apprehended. Payment will not be made for information leading to apprehension, nor for apprehension not followed by return to military control. Both reward and reimbursement may not be paid for the same apprehension and detention or delivery.

3. INDIVIDUAL CLAIMS HE/SHE IS NOT ABSENT WITHOUT AUTHORITY.

When a detained individual claims that he/she is not absent without leave and does not have the papers to prove his/her claim, the apprehending person or agency representative should communicate directly by the most rapid means available, with the nearest military installation manned by active duty personnel. When necessary, communicate directly (telephone or telegraph) with the Deserter Information Point of the military service concerned.

a. US Army:	U.S Army Deserter Information Point ATTN: ATZK-PMF-D 1481 Old Ironsides Avenue Fort Knox, KY 40121
Telephone:	Area Code (502) 626-3711/ 3712/3713
b. US Navy:	Navy Absentee Collection and Information Center (NACIC) 2834 Greenbay Road North Chicago, IL 60064
Telephone collect:	Area Code (847) 688-2106 (or toll free: 1-800-423-7633)
c. US Marine Corps:	Commandant, US Marine Corps Code POS-40 2 Navy Annex Washington, DC 20380-1775
Telephone collect:	Area Code (703) 614-3248/3376
d. US Air Force:	Headquarters AF Personnel Center (DPWCM) 550 C Street West, Suite 14 Randolph AFB, TX 78150-4716
Telephone collect:	Area Code (210) 566-3752 (or toll free: 1-800-531-5501)

APPENDIX (2)
OFFENSES IN AGGRAVATION OF DESERTION IN NAVAL SERVICE

Violations of the Uniform Code of Military Justice Article

82. Soliciting or advising another to: desert, mutiny, commit misbehavior before the enemy or engage in sedition.

90. Striking, drawing, or lifting up any weapon or offering any violence to his/her superior commissioned officer in the execution of his/her office.

91. Striking or otherwise assaulting a warrant officer, a noncommissioned officer or petty officer while in the execution of his/her office.

92. Disclosure of classified defense information.

93. Cruelty and maltreatment.

94. Mutiny or sedition.

95. Resistance, breach of arrest, and escape.

96. Releasing prisoner without proper authority.

97. Unlawful detention.

99. Misbehavior before the enemy.

100. Subordinate compelling surrender.

103. Looting and pillaging.

104. Aiding the enemy.

105. Misconduct as a prisoner.

106. Spying.

110. Improper hazarding a vessel.

113. Misbehavior of sentinel.

116. Riot.

118. Murder.

119. Manslaughter.

120. Rape.

122. Robbery.

124. Maiming.

125. Sodomy by force and without consent, or with a child under the age of 16 years.

126. Arson.

127. Extortion.

128. Assault upon a commissioned officer not in the execution of his/her office.

134. Assault:

a. Indecent.

(1) With intent to commit voluntary manslaughter, robbery, sodomy, arson or burglary.

(2) With intent to commit housebreaking.

(3) With intent to commit murder or rape.

b. Firearm, Discharging. Wrongfully and willfully, under/circumstances as to endanger life.

c. Homicide, Negligent. Indecent acts or liberties with a child under the age of 16 years.

d. Disloyal Statement. Impersonating a commissioned, warrant, noncommissioned or petty officer.

e. Obstruction of Justice.

f. Subornation of Perjury.

g. Communicating a Threat.

80. Attempting to commit any of the above.

81. Conspiracy to commit any of the above.

Any other offense within the investigative responsibilities of NCIS as prescribed by SECNAVINST 5430.107 to include cases involving desertion of officers and involving

personnel who have had access to classified defense information, which if disclosed, could jeopardize the security interests of the United States.

APPENDIX (3):
MEMORANDUM OF UNDERSTANDING BETWEEN UNITED STATES MARSHALS SERVICE AND NCIS (18SEP96)

U.S. Department of Justice

United States Marshals Service

Director

600 Army Navy Drive
Arlington, VA 22202-4210

September 18, 1996

MEMORANDUM TO: All U.S. Marshals Offices

FROM: (b)(6), (b)(7)(C)

SUBJECT: Memorandum of Understanding with Naval Criminal Investigative Service

On September 9, 1996, Director Roy D. Nedrow of the Naval Criminal Investigative Service (NCIS), and I signed a Memorandum of Understanding (MOU) regarding the Marshals Service and NCIS. The MOU combines resources for the apprehension of Navy deserters wanted for underlying crimes of violence and major drug offenses.

The attached MOU is a general guideline; the specific process outlined below will be in effect immediately.

NCIS Headquarters will provide Investigative Services Division (ISD) with a list of deserters who fit the criteria. ISD will notify the appropriate districts. The district will enter the deserter/fugitive into WIN/NCIC based on the underlying violent crime or drug charge. The district will then coordinate the investigation with the local NCIS office. A worldwide phone listing of all NCIS offices is attached.

Prior to each arrest the districts will coordinate with the local NCIS office to assume custody of the deserter/fugitive immediately.

Any questions concerning this MOU should be directed to Inspector (b)(6), (b)(7)(C)

THE UNITED STATES MARSHALS SERVICE
and
THE NAVAL CRIMINAL INVESTIGATIVE SERVICE

MEMORANDUM OF UNDERSTANDING REGARDING THE APPREHENSION OF VIOLENT FUGITIVES

I. GENERAL POLICY AND INTENT

This memorandum of understanding (MOU) provides general guidance with regard to working relationships between the United States Marshals Service (USMS) and the Naval Criminal Investigative Service (NCIS), regarding the investigation of certain fugitive matters and apprehension responsibilities. The intent of this MOU is to clarify and specify the role each law enforcement agency (as identified above) will play concerning the apprehension of certain fugitives who are the subjects of NCIS investigations for major felony offenses.

Key to this MOU is the sincere desire on the part of both agencies continuing to expand and make universal the close and mutually supportive relationships that widely exist among field components of both the USMS and NCIS. Additionally, each party to this agreement reasonably expects to achieve the more efficient utilization of existing agency resources by sharing common tasks and eliminating redundancy in fugitive apprehension efforts.

II. AUTHORITY TO CONDUCT INVESTIGATIONS

The statutory authority for the USMS and the NCIS to conduct criminal investigations, to include efforts to locate and apprehend fugitives from justice, include , but are not limited to:

USMS: Title 28, United States Code, Section 566; Department of Justice Violent Crime Initiatives; Title 28, Code of Federal Regulations, Section 0.111a.

NCIS: The Uniform Code of Military Justice; Title 10, United States Code, Sections 801-940; the Inspector General Act of 1978; Title 5, United States Code, Appendix 3 and section 301.

III. SPECIFIC POLICY AND PROCEDURES

- When the subject of the NCIS investigation has deserted from the military service and is wanted for a violent felony offense, major drug violation or any other special interest or significant crime. A violent felony is described as crime involving serious threat or injury to human life such as murder, rape, robbery, child molestation and offenses involving the use of firearms. Special interest or significant crimes include such offenses as major fraud, extortion, arson, property crimes. The USMS will not routinely seek the apprehension of military deserters unless he or she is also wanted for one of the crimes described above.

- When the subject of the NCIS investigation is a civilian or DoD dependent who is wanted under the circumstances described above and has fled the confines of the military installation.

- When the subject of an NCIS investigation is an active duty military member, civilian employee, or a dependent of an active duty military member or civilian employee who is wanted under the circumstances described above and is believed to be residing in a foreign country.

USMS National Crime Information Center entries will be coordinated at time of request for USMS investigative assistance. The Marshal Service will be the 24 hour contact for all warrant "hit" confirmations where the Marshal Service has provided investigative assistance to the NCIS.

IV. POST APPREHENSION GUIDELINES

Upon apprehension by the USMS of a fugitive wanted by the NCIS, the USMS and NCIS shall do the following:

- The USMS District office where the subject is arrested shall notify both USMS Headquarters and nearest NCIS component.

- The USMS will immediately contact NCIS Headquarters either telephonically or facsimile to inform them of the arrest.

- If possible, NCIS will arrange to assume custody of a military subject as soon as practical after the arrest. If NCIS is unable to assume custody of the military subject, the USMS agrees to remove the military subject via the USMS National Prisoner Transportation System (NPTS), at no cost to NCIS, to the responsible military installation where the prisoner will be turned over for further detention.

(b)(6), (b)(7)(C)

CODE	Agency Name	Address	Telephone Number
	NCIS Headquarters	716 Sicard Street	
CALE	NCISFO - CAROLINAS	1131 Chapel Crossing Road Building 305 Kiefer Circle	
SAC			
CACP	NCISRA Cherry Point, NC	Marine Corps Air Station Cherry Point PSC Box 8083	
CACS	NCISRA Charleston, SC	Charleston Naval Weapons Station 1661 Redbank Road, Suite 220	
CAPI	NCISRA Parris Island, SC	Marine Corps Recruit Depot Parris Island Post Office Box 5056	
CATD	NCISRA Camp Lejeune, NC	Marine Crops Base Camp Lejeue H-32 Julian C. Smith Boulevard	
DCWA	NCISFO - Washington Field Office	Building 200, Washington Navy Yard	
SAC			
DCAN	NCISRA Annapolis, MD	U.S. Naval Academy, Halligan Hall	
DCBE	NCISRU BETHESDA	8901 WISCONSIN AVENUE	
DCDL	NCISRU Dahlgren VA	17481 Dahlgren Road, Suite 103	
DCPX	NCISRA Patuxent River, MD	NAS Patuxent River 22514 McCoy Road, Building 463	
DCQV	NCISRA Quantico, VA	Marine Corps Base 3096 Range Road, Building 3096	
DCTS	NCISTSD Washington DC	Building 200, Washington Navy Yard	
DCVH	NCISPS NSA Washington DC-Hanover MD	Hanover, MD	
DCWA	NCISFO Washington DC	Building 200, Washington Navy Yard	

(b)(6), (b)(7)(C)

EUNA	NCISFO - Europe Field Office	Postal Service Center 817 Box 36
SAC		
EUAT	NCIS FDP Athens Greece	
EUAV	NCISRU Aviano	
EUGA	NCISRU Gaeta, Italy	Postal Service Center 811 Box 9
EUIS	NCIS FDP Tel Aviv Isreal	
EULD	NCISRU La Maddalena	
EULN	NCISRA London, England	Postal Service Center 821 BOX 41
EUML	NCISRU Malta	5800 Valletta Place
EUMO	NCIS FDP RABAT MOROCCO	
EUMS	NCISRU Marseille, France	Postal Service Center 116 (MAR)
EUPO	NCIS PSU Lisbon Portugal	PSC 807 BOX 77, FPO AE 09729-0077
EURM	NCISRU Rome, Italy	American Embassy PSC 59 Box 50
EURT	NCISRA Rota, Spain	Postal Service Center 819 BOX 35
EUSB	NCISRU Souda Bay, Greece	PSC 814 Box 18
EUSI	NCISRA Sigonella, Italy	Postal Service Center 812 BOX 3360
EUTE	NCISTSD Europe Rota Spain	PSC 817, BOX 36, FPO AE 09622
EUVE	NCISPS Europe Italy	PSC 817, BOX 36, FPO AE 09622
FEYK	NCISFO - Far East Field Office	Building 1997, Yokosuka Naval Base

(b)(6), (b)(7)(C)

(b)(6), (b)(7)(C)

SAC	(b)(6), (b)(7)(C)		
FEAJ	NCISRA Atsugi, Japan	Postal Service Center 477 BOX 8	
FECN	NCISRU Chinhae, Korea	COMFLEACT	
FEIW	NCISRA Iwakuni, Japan	Building 608, Marine Corps Air Station Misumi-Cho, Iwakuni City, Japan 740-0025 Postal Service Center 561 BOX 71	
FEMW	NCISRU Misawa, Japan	UNIT 5051	
FEOK	NCISRA Okinawa, Japan	UNIT 35021	
FEPU	NCISRU Pusan, Korea	Building 119, Taegu (K-12)	
FERK	NCISRA Seoul, Korea	Building 2680, U.S. Army Garrison UNIT 15250	(b)(6), (b)(7)(C)
FESS	NCISRA Sasebo, Japan	Postal Service Center 476 BOX 75	
FEVK	NCISPS Okinawa, Japan	NCIS Polygraph Site, Unit 35021, FPO AP 96673--5021	
FEXV	NCISRU USS Kitty Hawk	Naval Criminal Investigative Service Special Agent Aloat USS Kitty Hawk (CV63)	
GCPF	NCISFO Central - Gulf Coast Pensacola FL	341 Saufley Street	
SAC	(b)(6), (b)(7)(C)		
GCCA	NCISRU Crane, IN	Naval Weapons Support Center 300 Highway 361, Building 12	
GCCC	NCISRA Corpus Christi, TX	Corpus Christi Naval Air Station 385 Southeast Fift Street, Suite 2A	
GCCL	NCISRU Cleveland, OH	Post Office Box 99809	
GCDA	NCISRA Dallas, TX	Naval Air Station 2201 North Collins Street, Suite 350	

GCGF	NCISRU Gulfport MS	Gulfport Naval Construction Battalion Center Number 213, Building 60	
GCGL	NCISRA NTC Great Lakes, IL	Great Lakes Naval Training Center 2540A Paul Jones Street	
GCMT	NCISRA Memphis, TN	Memphis Naval Air Station 5722 Integrity Drive	
GCNR	NCISRA New Orleans, LA	New Orleans Naval Support Activity 2300 General Meyer Avenue	
GCPA	NCISRU Pascagoula, MS	Post Office Box 1652	
GCPC	NCISRU Panama City, FL	6703 West Highway 99, Suite 385B	
GCSL	NCISRA Saint Louis, MO	National Personnel Records Center Post Office Box 12408	
GCTP	NCISPS Pensacola, FL	Pensacola Naval Air Station 341 Saufley Street	
GCVP	NCISTSU Pensacola, FL		
HIHN	NCISFO - Hawaii Field Office	Pearl Harbor Naval Station 449 South Avenue	
SAC	DIPRIZIO, CHERYL A.		
HIKH	NCISRA Kaneohe, HI	Marine Corps Barracks Hawaii 1096 Second Deck Post Office Box 63070	
HIHM	NCISRA Marianas, GU	Commander Naval Forces MarianasBuilding 2, Second Floor	
HITH	NCISTSD Pearl Harbor HI	160 Keen Road, Pearl Harbor, HI 96860	
HIVI	NCISPS Pacific-Pearl Harbor HI	449 South Avenue, Pearl Harbor, HI 96860-4988	
MEBJ	NCISFO - Middle East Bahrain	PSC 451 Box 400, FPO AE 09834-2800	
SAC	WINSLOW, EDMUND T.		
MEDB	NCISRA Dubai, United Arab Emirates	6020 Dubai Place, Attn: RAC Einsel, Dulles, VA 20189	
MEDJ	NCISRA Sana'a, Yemen	US Embassy, Attn: FPD, 6330 Sana'a Place	

(b)(6), (b)(7)(C)

MEKU	NCISRA Kuwait City, Kuwait	Camp Patriot	
MPMP	NCISFO - Southeast Field Office	Mayport Naval Station Post Office Box 280076	
SAC	KISTHARDT, CAROL		
MPAB	NCISRU Albany, GA	Marine Corps Logistic Base Albany 814 Radford Boulevard, Suite 20310	
MPKW	NCISRU Key West, FL	P.O. Box 9020 NAS	
MPGT	NCISRA Guantanamo Bay, Cuba	Guantanamo Bay Naval Station PSC 1005 Box 42	
MPJX	NCISRA Jacksonville, FL	Jacksonville Naval Air Station Post Office 58	
MPMC	NCISRU Miami, FL	Homestead Air Force Base 12700 Tuskegee Blvd	
MPKB	NCISRA Kings Bay, GA	Kings Bay 1342 USS Simon Bolivar Road	
MPSJ	NCISRU San Juan Puerto Rico	Puerto Rico Branch Office (CID) 3D MP GP CID USACIDC	
MPPZ	NCISREP Panama City Panama	Unit 0945 (FPD), APO AA 34002	
MPRL	NCISRU Orlando, FL	12359 Research Parkway	
MPTA	NCISRU Tampa, FL	4815 N. Hubert Avenue, Rm 112	
MPTM	NCISTSD Jacksonville, FL	P.O. Box 58, NAS	
MPVJ	NCISPS Jacksonville, FL	PO BOX 58, NAS, Jacksonville Fl, 32212	
MWPE	NCISFO - Marine Corps West Field Office	Marine Corps Base Camp Pendleton Building 1224, Post Office Box 555238	
SAC	COTE, CHRISTOPHER		
MWTN	NCISRA Twenty-Nine Palms, CA	Marine Corps Ground Combat Center Twenty-Nine Palms Post Office Box 788117	

(b)(6), (b)(7)(C)

MWMM	NCISRA Miramar, CA	Marine Corps Air Station Miramar Post Office Box 452138
MWVD	NCISPS SAN DIEGO, CA	BOX 555238, Camp Pendelton CA
MWYU	NCISRA Yuma, AZ	Marine Corps Air Station Yuma Post Office Box 12366
NENP	NCISFO - Northeast Field Office	Newport Naval Education & Training Center 344 Meyerkord Avenue, Suite 3
SAC	NIGRO, ROBERT M.	
NEBK	NCISRA Brunswick, ME	2252 ORION STREET, BRUNSWICK, ME 04011
NEEA	NCISRA Earle, NJ	Earle Naval Weapons Station 201 South Highway 34, Building C8
NELH	NCISRA Lakehurst, NJ	Lakehurst Naval Air Warfare Center Post Office Box 1108
NEMB	NCISRU Mechanicsburg, PA	Mechanicsburg Navy Inventory Control Police5450 Carlisle Pike, Building 112
NENL	NCISRA New London, CT	Groton Naval Submarine Base Post Office Box 30
NENY	NCISRU New York-Brooklyn, NY	201 Varick Street, Room 1009
NEPB	NCISREP Pittsburg, PA	US Dept of Energy Pittsburgh Naval Reactors Office, P.O. Box 109
NEPN	NCISRU Portsmouth, NH	Portsmouth Naval Shipyard Building H-29
NESC	NCISREP Schenectady, NY	DOE P.O. Box 1069 (Attn: NCIS)
NEVL	NCISPS New London CT	
NEUP	NCISREP University Park, PA	Applied Research Laboratory, Garfield Thomas Water Tunnel, RM 217A, (Attn: NCIS)
NFNF	NCISFO - Norfolk Field Office	1329 Bellinger Boulevard
SAC	WORTH, SAM	
NFCE	NCISRU Oceana, VA	Oceana Naval Air Station 799 Hornet Drive., Suite 150

NFPV	NCISRU Portsmouth, VA	Portsmouth Naval Shipyards Building M32
NFHV	NCISRU USNH Portsmouth, VA	620 John Paul Jones Circle
NFLC	NCISRU Little Creek, VA	Little Creek Naval Amphibious Base1450 7th Street, Building 3175
NFFM	NCISRFU Fraud Unit	825 I Greenbrier Circle
NFLT	NCIS STAA Little Creek, VA	1430 Helicopter Road, Suite 250
NWBG	NCISFO - Northwest Field Office	Land Title Professional Building 9657 Levin Road, NW; Suite L20
SAC	(b)(6), (b)(7)(C)	
NWBR	NCISRA Bremerton, WA	Kitsap Naval Base 2240 Decatur Avenue, Building 506
NWEV	NCISRA NAVAL STATION EVERETT WA	2000 W. MARINE VIEW DRIVE BLDG 2000 - RM 234 EVERETT, WA 98207
NWTG	NCISTSD BANGOR WA	TECHNICAL SERVICES DETACHMENT LAND TITLE PROFESSIONAL BUILDING 9657 LEVIN RD NW STE. L20 SILVERDALE, WA 98383
NWVB	NCISRA Everett, WA	Everett Naval Station 2000 West Marine View Drive
NWWH	NCISRA Whidbey Island, WA	Whidbey Island Naval Air Station 975 West Forrestal Street
NWXJ	NCISRU USS JOHN C. STENNIS (CVN-74)	BOX 81, FPO AP 96615-2874
NWXL	NCISRU USS Abraham Lincoln (CVN-72)	FPO AP 96612-2872
SNSN	NCISFO - Sinapore Field Office	Personnel Support Activity Sembawang Wharves Building 7-4, Deptford Road
SAC	(b)(6), (b)(7)(C)	
SNSN	NCISRA APD Singapore	Postal Service Center 470 BOX 2900

(b)(6), (b)(7)(C)

SNMQ	NCISRA/FPD Manila, Philippines	Postal Service Center 500 BOX 23
SNAS	NCISRA/FPD Sydney, Australia	Force Protection Detachment, US Consulate General
SNPR	NCISRU/FPD Perth, Australia	Force Protection Detachment, Perth, Unit 11021
SWND	NCISFO - Southwest Field Office, San Diego	3405 Welles Street, Suite 1 Post Office Box 368130
SAC		
SWCK	NCISRA China Lake, CA	China Lake Naval Air Weapons Station Building 00451
SWCO	NCISRU Corona, CA	Corona Naval Surface Warfare Center 2300 Fifth Street, Building 515
SWDM	NCISREP Davis Monthan AFB AZ	5345 E. MADERA STREET BLDG 4310, ROOM 318/320 DAVIS MONTHAN AFB TUCSON, AZ 85707
SWFL	NCISRU Fallon, NA	Fallon Naval Air Station Building 427
SWLA	NCISRA Los Angeles, CA	800 Seal Beach Boulevard, Building 254
SWLM	NCISRA Lemoore, CA	Lemoore Naval Air Station 838 Hancock Circle
SWMY	NCISRU Monterey, CA	1870 Morse Drive
SWPH	NCISRA Venture CA	4111 SAN PEDRO STREET 2ND FLOOR EAST
SWPT	NCIS STAAT San Diego CA	Building 91, NB Coronado
SWTC	NCISTSD San Diego CA	33077 Ping Place Ste 101, San Deigo

(b)(6), (b)(7)(C)

(b)(6), (b)(7)(C)

CHAPTER 3
TITLE: THREAT MANAGEMENT UNIT (TMU)
POC: CODE 23
DATE: JAN 2010

3-1. INTRODUCTION

3-1.1. General. In 1996, the Naval Criminal Investigative Service (NCIS) established the Threat Assessment Unit at NCIS Headquarters (NCISHQ). The Threat Assessment Unit was established due to a noticeable increase in national and Department of Navy (DON) incidents of workplace violence, stalking, and threatening communications. The name of the Threat Assessment Unit was subsequently changed to the Threat Management Unit (TMU). The TMU is located within the Criminal Investigations Directorate (Code 23). It should be understood that TMU assistance/ guidance can and should be used by all disciplines (General Criminal, Counterintelligence, Combating Terrorism, and for NCIS internal investigations). Many people equate a TMU solely with domestic violence or workplace violence. The services provided by the TMU cover a wide range of topics, including, but not limited to terrorism, school violence, sexual crimes, stalking, cyber crimes (cyber stalking), domestic violence, arson, sabotage, communicated threats, insider threats, pre-attack behavior and a myriad of other incidents.

3-1.2. Purpose. The TMU was established to provide criminal and behavioral analysis and risk assessments for NCIS investigations in an attempt to review, and ultimately mitigate, the potential for violence. The TMU is a multidisciplinary support team made up of special agents, staff psychologists, analysts and others. Investigative analysis provided by the TMU includes violence risk assessments, interview and interrogation strategies, and management plans. It is important to understand that the role of the TMU is multifaceted. The information provided by the TMU can help agents in the field with complex and possibly volatile investigations. The TMU will assist the field in achieving resolutions to these investigations with the main goal being to prevent violence, injury, or other damaging outcomes. The TMU can also provide information pertaining to agent safety during the course of these often dangerous and volatile investigations.

3-2. PROGRAM ADMINISTRATION

3-2.1 NCIS Headquarters TMU. The TMU personnel located at NCISHQ are subject matter experts in threat assessment and violence prevention issues. Most of the NCIS Field Offices (FO) have one or more FO TMU representatives who are trained by TMU Headquarters personnel to understand the dynamics of potentially threatening and volatile investigations. If the special agent in the field has an investigation that could benefit from a TMU consultation, they should contact their local FO TMU representative who will work closely with the TMU headquarters personnel. The names of the FO TMU representatives can be found on the NCIS Criminal Investigations & Operations Directorate website under the TMU homepage (http://infoweb.ncis.navy.mil/agency/deptwebsites/crim/crim-tmu.html). The TMU, when contacted early on in an investigation, can assist in facilitating a quality investigation and preventing future violence.

3-2.2. In addition to assisting field agents with complex and sometimes volatile investigations, the NCISHQ TMU maintains a database of unsolicited communications. Unsolicited communications are defined as threatening, harassing, or otherwise concerning communications sent to Department of the Navy (DON) leadership, command leadership, or other persons within a command. The communications may or may not include threatening statements. Communications may be handwritten, computer generated, photocopied documents, audio visual tapes, CDs, DVDs or electronic files. All unsolicited communications shall be forwarded to the TMU, NCISHQ Code 23B1 for inclusion in the Unsolicited Communications Database. At this point in time, only NCISHQ TMU personnel have access to the Unsolicited Communications Database. When applicable, HQ TMU personnel can query the database in reference to NCIS investigations.

a. If the field agent and/or their supervisor believe the unsolicited communication contains a threat that is specific and requires immediate action, an investigation will be opened and coordination with the TMU should occur at the onset. Field agents or supervisors should contact either their FO TMU Representative or TMU personnel at NCISHQ via telephone as soon as practicable. As stated above, TMU personnel can be identified by accessing the NCIS Criminal Investigations & Operations Directorate website under the TMU page. Examples of threats that require immediate action are those that contain very specific, detailed information which appear to have credibility. (If an agent is unsure about the potential threat, coordination should be made immediately with the NCISHQ TMU for review of the specificities of the threat). If the communication involves a DoD/DON senior under NCIS Protective Service Operation (PSO) protection, PSO should also be immediately notified. NCISHQ TMU will review the Unsolicited Communications Database to ascertain if similar communications have been received in the past. The threatening communication should be forwarded to NCISHQ TMU immediately as a scanned attachment to an e-mail. If this is not possible, it should be faxed to NCISHQ.

b. The communication will subsequently be appended as an enclosure to an Investigative Action (IA) if an investigation is initiated. If the communication does not include a threat, (e.g., rambling, incoherent comments), an investigation does not need to be initiated, but the communication must still be forwarded to the NCISHQ TMU for inclusion in the database.

3-2.3. Field Office Threat Management Representatives. Each NCIS field office has one TMU representative. The field office TMU representative is a collateral duty and the representative is acting in this capacity in order to assist local field office agents when complex and possibly dangerous or escalating investigations are initiated. The field office TMU representative shall act as a conduit between NCISHQ TMU and agents in the field. Some of the roles and responsibilities of the FO TMU representatives are listed below.

a. Work closely with the NCISHQ TMU personnel. When necessary, the FO TMU representative will coordinate with NCISHQ TMU personnel concerning risk assessments, criminal and behavioral assessments, interview/interrogation strategies, and approach techniques for qualifying field office investigations.

b. Provide training to local commands and to the agents within their area of responsibility (AOR) on issues involving threat assessment (e.g., workplace violence).

c. Provide recommendations to FO special agents regarding investigative strategies and security related solutions for specific TMU investigations.

d. Must maintain close liaison with Family and Sexual Violence (F&SV) agents and assist in identifying couples/individuals who are at high risk for escalating violence. The field office TMU representative should be familiar with local social service resources, such as women's shelters, etc.

e. The field office TMU representatives are well trained in TMU related strategies and issues by the NCIS HQ TMU personnel. FO TMU personnel may also receive outside training when available. They should stress and ensure that agents within their AOR maintain close relationships with local victim advocates and others who can assist in preparing safety plans. The field office TMU representative can help coordinate obtaining Orders of Protection.

f. NCISHQ TMU personnel will provide updated information to the field office TMU representatives when it pertains to any TMU related areas of interest or when changes or updates are implemented.

3-3. TMU POLICY

3-3.1. Threats of Violence. All threats of violence will be addressed immediately by both the FO TMU representative and NCISHQ TMU. NCISHQ TMU will respond promptly to requests for assistance/guidance regarding threat assessments. For immediate coordination, TMU personnel (HQ and/or FO) should be contacted telephonically.

3-3.2. TMU Assessments. Assessments or any type of documentation provided to the case agent from the TMU is to be utilized by the case agent as "case notes" and may not be attached to any external reports without TMU approval. The information provided by the TMU can be used to verbally brief commands and other concerned parties.

3-3.3. In order to facilitate a timely and comprehensive assessment when assistance is requested of the NCISHQ TMU, the case agent should supply photocopies of all case information and

correspondence, along with copies of all audiotapes, videotapes, transcripts and other pertinent information to Code 23B1 as expeditiously as possible. The quality of the analysis will be a direct result of the quality of the submitted data, therefore the field agents should provide detailed submissions for review by the TMU.

3-3.4. Any time an agent in the field contacts the TMU, an annotation will be made in the Case Activity Record (CAR), indicating TMU liaison was made, and with whom. The annotation will also be made in the next ROI (Interim) that is prepared.

3-4. TMU PROGRAM

3-4.1. TMU Functions

a. The TMU, in coordination with the case agent, can assess the risk of violence posed by a specific offender. NCISHQ TMU can provide feedback to the field based on information developed after NCISHQ TMU personnel contact the field agent(s) and receive details pertaining to the actual or implied threat. This is especially important in domestic violence, workplace violence, school violence and stalking investigations. Appendix (1) is a list of security recommendations for various settings (home, office, and vehicle). In addition to providing this list to a victim, the case agent shall review the contents of the document with the victim and answer any safety questions that might arise. Appendix (2), a stalking incident log, can be provided to victims who claim they are being stalked. The victim can annotate each stalking event by listing the date and time, place, jurisdiction (responding officer), and incident. Many stalking incidents cross jurisdictional lines. This allows the victim and law enforcement to have a detailed list of the type and frequency of events.

b. The NCISHQ TMU can assist in narrowing a subject pool and identifying perpetrators in unknown subject cases, especially in homicides, arson, and sabotage cases.

c. When a dangerous situation or a risk of violence situation is identified, the TMU can develop a management plan to mitigate future risk for violence.

d. Subsequent to coordination with the TMU, it is very important that the case agent continually brief the command concerning any potential dangers or risks involving the alleged suspect.

3-4.2. Communicated Threats. Threats should always be taken seriously and be fully investigated.

a. The depth of the investigation depends on several factors, including, but not limited to, the facts of the case, threats made (specific, vague, through a second party, etc.), the ability of the alleged subject to carry out the threat, and the mental health of the subject.

b. The FO TMU representative shall be contacted/consulted to determine if an investigation should be opened or the situation merely monitored. If you are unable to contact the FO TMU representative, contact TMU at NCISHQ for assistance.

3-4.3. Threat Assessments. The threat assessment helps NCIS special agents and others assess, manage, and understand situations involving a potential risk or potential risk of violence. Special agents should be keenly aware of escalating violent behavior. Investigations that show increasing violence risk are excellent candidates for TMU coordination. Investigations involving patterns of behavior (e.g., letter writing, phone calls, following a person, giving gifts, etc) are other instances wherein TMU consultation would be helpful to the case agent. In addition to threat assessments, interview and interrogation strategies, risk assessments, and victim safety plans can also be useful TMU support tools for the case agent.

3-4.4 Victim Safety Plans. Victim safety plans are prepared on a case by case basis by TMU HQ personnel, the case agent, and sometimes will include input from the victim. Many parts of a victim safety plan are victim specific and what is appropriate for one victim may not be appropriate for another victim. The victim safety plan is a collaborative effort and it is sometimes dynamic and can change during the course of an investigation. Case agents in the field can verbally brief a victim concerning a safety plan or on other occasions the safety plan provided by NCISHQ TMU may be in writing. If a written safely plan is provided to a field agent, that document will be handled as case agent notes and will not be appended to any report. The case agent shall work with the victim to ensure the safety plan is appropriate for the specific victim and circumstances. The victim safety plan should be updated as needed.

3-4.5. Aggravating Factors. Drug and alcohol use by the suspect, mental illness, owning or having access to weapons, past criminal history, past violent history, and/or past suicide attempts or gestures are all factors which can suggest an increased risk for future violence.

3-4.6. Requesting Assistance from TMU. When requesting TMU support or assistance, as much information as is known should be shared with the TMU. When a risk assessment is requested on a specific person, it is critical that all details pertaining to that person be provided to the TMU. The following information about the alleged perpetrator and incident(s) should be provided to the TMU if known:

a. Full biographical data.

b. Detailed background of the investigation, including the results of all database checks. (NCIC, DCII, JPAS, LInX, CLEOC, NLETS, FAP, etc). Checks will also be made of the NCISHQ TMU Unsolicited Communication Database.

c. Full educational background to include highest grade completed.

d. Present employment, employment history, military background, and/or specialized training.

e. Marital status and family make up.

f. History of weapons use. For example, does the person have weapons training from the military, law enforcement, etc? Ascertain if the person has any weapons registered to him/her by checking either on base or with local law enforcement.

g. Review the Service Record Book (SRB) if applicable.

h. Nature of the relationship between victim and subject.

i. Description of the conflict between the victim and subject.

j. Subject's history of violence against this victim and against others.

3-5 INVESTIGATIONS

3-5.1. The TMU can work with, and should be considered by any discipline within NCIS. Even though the TMU is most often associated with Code 23 (Gen Crim), their assistance and expertise can be of great value to Code 21 (Combating Terrorism Directorate), Code 22 (Counterintelligence Directorate), Multiple Threat Alert Center (MTAC), Protective Services (unsolicited threats and communications made to principals), the Office of Special Projects, and the NCIS Inspector General's Office.

3-5.2. Many different criminal investigations can benefit from a TMU consultation. Cases that involve a risk for future violence often benefit from TMU consultation. These cases include stalking, workplace violence, domestic violence, school violence, and communicated threats. Additionally, cases which involve pre-attack behaviors may also benefit from TMU consultation, including sabotage, wrongful destruction, arson, burglary, larceny, assault, death investigations, sex offenses, and missing persons. All of the offenses and criminal elements for the above listed case categories are discussed in various chapters within NCIS-3.

3-5.3. Violent or dangerous behavior can lead to other crimes or disturbing incidents allowing the situation to escalate, encompassing more violations of the Uniform Code of Military Justice and/or local statutes. For example, while investigating a serious domestic violence case, the special agent must be mindful that the suspected perpetrator might begin to stalk the victim. The stalking can include behavior such as harassing phone calls, vandalism, threats (verbal, written), voyeurism, trespassing, violation of protective orders, assault, larceny (stealing personal items), burglary, arson, and even homicide. It is important to keep in mind that other criminal incidents which might occur during the conduct of the primary investigation may be interrelated with the primary offense.

3-5.4. During stalking investigations, it is important to account for all of the behaviors the subject has demonstrated against the victim. Minor or annoying behaviors (e.g., hang-up" phone calls, keying a car, or pouring sugar into a car gas tank) should not be discounted or overlooked.

3-5.5. Many criminal cases wherein TMU assistance/review has been requested also necessitate close coordination with local victim advocates, family advocacy case managers, and/or sexual assault intervention specialists. It is important that NCIS special agents keep advocates and counselors apprised of TMU risk assessment information, for the victim's protection and safety.

3-6 TMU CONSIDERATIONS

3-6.1. When coordinating with the TMU, be mindful of the previously discussed potential aggravating factors, such as drug use, alcohol use, mental illness, availability of weapons, past criminal history (especially violent incidents), and past suicide attempts or ideations. These details should be provided to the TMU as soon as possible, to assist with the threat assessment process.

3-6.2. It is also imperative that the case agent provide all details surrounding the alleged incidents(s) no matter how minor or inconsequential. The information could be important for the TMU to develop and show escalation of events.

3-6.3. The TMU has developed an interview protocol to assist the field agent with interviewing victims and witnesses, and during the interrogation of subjects. Appendix (3) contains information and guidance to field agents who will be conducting interviews or interrogations on cases that might generate TMU involvement (there is no threshold establishing a level to meet TMU involvement). The TMU at NCISHQ can assist the agent in developing appropriate questions for the investigation, using biographical and historical data previously provided by the case agent.

a. Ascertain the type of relationship the victim (interviewee) has with the alleged subject (if subject has been identified). Is the interviewee a co-worker, spouse, girlfriend/boyfriend, acquaintance, family member, etc, or is there no known relationship?

b. Question the interviewee concerning the frequency of incidents and when they started.

c. Obtain full details as to the behavior involved: stalking, harassing phone calls, vandalism, etc.

d. Obtain full details concerning comments or actions made by the alleged suspect.

e. Ascertain how many potential victims there are.

f. Question the interviewee about any “aggravating” factors that may be involved (drug abuse, intoxication, mental health issues, access to weapons, etc).

g. Question the interviewee in detail concerning each individual incident, do not ask general questions. Each incident must be reviewed on its own.

h. Interview all known/available associates of the alleged suspect, including but not limited to family members, co-workers, fellow students, and friends.

i. Make sure the interview and subsequent statement contains details about all the criminal offenses that may have occurred, including details that can prove the elements of the offense(s). For example, in a “communicating a threat” investigation, provide specifics as to how the threat was delivered (phone, e-mail, letter, in person, etc), provide the exact threatening language, if possible,

and address the ability of the suspect to carry out the threat. This would include if any weapons were available or present when a threat was made.

j. Make sure the interviewee is aware of and familiar with their safety plan, including their knowledge of how to contact first responders if necessary. (Safety plans should be implemented at the beginning of these investigations and are often created with assistance and input from FAP or a victim advocate).

3-6.4. Subject Interrogation Protocol. Just like the victim/witness interview protocol, the NCISHQ TMU can also prepare a subject interrogation protocol for the case agent. Remember, when advising the subject of his/her rights, be certain to include all known offenses. (For example, if working a "workplace violence" investigation, you may read rights for "assault," "communicating a threat," and "indecent acts." There is no actual crime called "workplace violence.")

a. It is best that the interrogation of the alleged suspect is coordinated through the NCISHQ TMU when there has been prior case coordination with the TMU.

b. The TMU can assist in providing the case agent with an interrogation protocol. It is best to have as much detailed information on the alleged suspect as possible before the suspect is interrogated.

c. Question the alleged suspect about each and every incident/crime that is being investigated. Do not just have all the incidents (if more than one) as an aggregate to which the suspect will then provide just one answer.

d. Due to the violent nature of most of the incidents involving TMU assistance, it is imperative that the case agent be overly cautious in reference to agent safety.

3-7. TARASOFF WARNINGS (DUTY TO WARN)

3-7.1 Tarasoff v. Regents of the University of California, 1976, was a case in which the Supreme Court of California held that **mental health professionals** have a duty to protect individuals who are being threatened with bodily harm by a patient. The original 1974 decision mandated warning the threatened individual, but a 1976 rehearing of the case by the California Supreme Court called for a "duty to protect" the intended victim. Per the ruling, the mental health professional may discharge the duty in several ways, including notifying police, warning the intended victim, and/or taking other reasonable steps to protect the threatened individual. This decision has since been adopted by most states in the U.S. and is widely influential in jurisdictions outside the U.S. as well.

3-7.2. 'Tarasoff' is a general term, referring to a body of case law, which applies when a client directly communicates to a mental health professional a serious threat of physical violence against a reasonably identifiable victim.

a. Tarasoff imposed an affirmative duty on **mental health workers** that the right to confidentiality ends when the public peril begins. Failure to act may also result in potential civil

liabilities. The mental health professionals have to establish four parameters: type of harm, seriousness of harm, imminence of harm, and likelihood of harm.

b. The mental health professional must make reasonable efforts to communicate this threat both to the reasonably identifiable victim(s) and the law enforcement agency where the client lives.

c. NCIS special agents should have awareness and familiarity with the guidelines pertaining to the "duty to warn" (Tarasoff). Special agents may be contacted by a mental health professional regarding serious and/or imminent potential harm perpetrated either by or on someone associated with the DON. Agents must understand that the doctor/client privilege is outweighed by the court imposed "duty to warn". Tarasoff is not applicable to NCIS special agents, only mental health professionals.

APPENDIX (1): NCIS THREAT MANAGEMENT UNIT (TMU) SECURITY GUIDELINES

NCIS Threat Management Unit: Victim Security Recommendations

Residence Security

1. Be alert for any suspicious persons.
2. Positively identify individuals before opening doors. Install a wide angle viewer in all primary doors.
3. Install a porch light at a height that would discourage removal.
4. Install dead bolts on all outside doors. If you cannot account for all previous keys, replace all door locks. If you are renting a residence, insist on the replacement of all door locks. Secure spare keys. Place a dowel in sliding glass doors and all sliding windows.
5. Keep garage doors locked at all times. Keep car doors secured at all times, even when the car is in the garage. Use an electric garage door lock.
6. Install adequate outside lighting. Consider motion detector lighting, which can discourage intruders.
7. Trim shrubbery around windows and doorways. Install locks on fence gates.
8. Keep fuse box locked. Have battery lanterns in residence.
9. Install a loud exterior alarm bell that can be manually activated from more than one location
10. Maintain an unlisted telephone number. Alert household members to unusual and wrong number calls. If such activity continues, notify a local law enforcement agency. Maintain a log of all such calls, to include the dates, times and the content of the calls.
11. Any written or telephone threat received should be saved and forwarded to the appropriate law enforcement authorities.
12. All firearm(s) should be kept out of reach of children.
13. Household staff should have a security check prior to employment and should be thoroughly briefed on security precautions. Strictly enforce a policy of the staff not discussing family matters or movements with anyone.
14. All household members should be alert for any unusual or suspicious packages, boxes, or devices on the premises. Do not attempt to open or in any way disturb such objects.
15. Maintain all-purpose fire extinguishers in the residence and in the garage. Install a smoke detector system and carbon monoxide detectors throughout the residence.
16. Tape all emergency telephone numbers on all telephones, to include cordless handsets.
17. When away from the residence for an evening, place lights and radios on a timer. For extended absences, arrange to have deliveries suspended.
18. Keep all doors and windows secured, even while in residence.
19. Prepare an evacuation plan. Brief household members on plan procedures. Provide ladders or rope for two and three story residences.
20. A family dog is one of the least expensive and most effective deterrents.
21. Know the whereabouts of all family members at all times.
22. Children should be accompanied to school or bus stops.
23. Routes taken and time spent walking should be varied.
24. Require identification of all repairmen and salesmen prior to permitting entry.
25. Always park in a secured garage, if available.

26. Inform a trusted neighbor regarding the situation. Provide the neighbor with a photo or description of the suspect and any possible vehicles.
27. Stop delivery of all mail and newspapers when going away on extended vacations, or have a trusted neighbor pick up these items.
28. If residing in an apartment complex, provide the on-site manager with a picture of the suspect. If in a secured condominium, provide information to the doorman or valet.

Office Security

1. Central reception should handle visitors and packages.
2. Office staff should be alerted to suspicious people, parcels and packages that do not belong in the area.
3. Establish key and lock controls. If keys possessed by terminated employees are not retrieved, change all locks.
4. Park in secured area if at all possible
5. Have names removed from any reserved parking area.
6. If there is an on-site security director, inform them of the situation. Provide security with a photograph (if possible) of the suspect, the vehicle, or a detailed description.
7. Have a secretary or co-worker screen calls, if necessary.
8. Have a secretary or security personnel screen all incoming mail (personal) or fan letters.
9. Be aware of anyone possibly following you from work.
10. Do not accept any packages unless you personally order an item.

Vehicle Security

1. Park vehicles in well-lit areas. Do not patronize lots where car doors must be left unlocked and keys surrendered; otherwise leave only the ignition key. Only allow items to be placed in or removed from your vehicle in your presence.
2. When parked in the residence garage, turn the lights on and lock the vehicle and garage door.
3. Equip the gas tank with a locking cap. The hook locking device should be controlled from inside the vehicle.
4. Visually check the front and rear passenger compartments before entering the vehicle.
5. Select a reliable service station for vehicle service.
6. Keep doors locked while the vehicle is in use.
7. Be alert for vehicles that appear to be following you. If you do suspect someone is following you, do not return to your home; drive to the nearest police or fire station. Sound the horn to attract attention.
8. When traveling by vehicle, plan ahead. Know the locations of police stations and fire departments.
9. Use a different schedule and route of travel each day.
10. Do not stop to assist stranded motorists. Do not pick up hitchhikers.
11. Have your keys in hand before entering a parking garage or parking lot.
12. Keep all vehicle doors and windows secured.
13. Leave sufficient room between you and another vehicle during stops, so that you are able to turn out of the lane if needed.

Personal Security

1. Remove home address on personal checks and business cards. Remove social security number from personal checks.
2. Place real property in a trust, and list utilities under the name of the trust.
3. Utilize a private mail box service to receive all personal mail.
4. File for confidential voter status or register to vote utilizing mailbox address.
5. Destroy discarded mail.
6. Telephone lines can be installed in a location other than the person's residence and call-forwarded to the residence.
7. Place residence rental agreements in another person's name.
8. Your name should not appear on service or delivery orders to the residence.
9. Remove all signs on your residence with your name (e.g., mailboxes, doorways).
10. Do not leave your name on your answering machine at your residence.

APPENDIX (2): STALKING INCIDENT LOG:

Stalking Incident Log for _____

Date:	Time:	Incident Type:	Officer: Name/Phone: Badge #:	Report #: Location (home/work/ car, etc.): Name:	Incident:	Witness Information Name: Address: Phone:
Date:	Time:	Incident Type:	Officer: Name/Phone: Badge #:	Report #: Location (home/work/ car, etc.): Name:	Incident:	Witness Information Name: Address: Phone:
Date:	Time:	Incident Type:	Officer: Name/Phone: Badge #:	Report #: Location (home/work/ car, etc.): Name:	Incident:	Witness Information Name: Address: Phone:
Date:	Time:	Incident Type:	Officer: Name/Phone: Badge #:	Report #: Location (home/work/ car, etc.): Name:	Incident:	Witness Information Name: Address: Phone:

Date:	Time:	Incident Type:	Officer: Name/Phone: Badge #:	Report #: Location (home/work/ car, etc.): Name:	Incident:	Witness Information Name: Address: Phone:
Date:	Time:	Incident Type:	Officer: Name/Phone: Badge #:	Report #: Location (home/work/ car, etc.): Name:	Incident:	Witness Information Name: Address: Phone:
Date:	Time:	Incident Type:	Officer: Name/Phone: Badge #:	Report #: Location (home/work/ car, etc.): Name:	Incident:	Witness Information Name: Address: Phone:
Date:	Time:	Incident Type:	Officer: Name/Phone: Badge #:	Report #: Location (home/work/ car, etc.): Name:	Incident:	Witness Information Name: Address: Phone:

APPENDIX (3): Victim Interview Protocols

Victim Interview Protocol

1. Identify type of relationship
    - Family member Relationship: _____
    - Acquaintance _____
    - Co-worker _____
    - Other _____

2. Chronology
    - Length of time subject behavior (assault, stalking etc) has been occurring _____
    - Frequency of behavior _____
    - When did the behavior start _____

3. Collect 911 tapes
    - Who called 911? _____
    - Why? _____
    - Are there children in the home? No____ Yes ____
    - Have the children been victims and/or witnesses of the subject's behavior? ____

4. Identify Risk Indicators
    - Substance Abuse No ____ Yes ____
    - Prior threats of bodily harm No ___ Yes ___
      (If yes, expand) _____
    - Threats of suicide No____ Yes _____
    - History of weapons possession No ___ Yes ___
    - Arrest History No ____ Yes _____(details)

5. Documentation of each incident
    - Direct threat or implied threat? ___
    - The tone of the statement? ___

6. Photograph injuries over several days, make sure you mark the dates

7. Victim Sign waivers
    - Medical ____
    - Dental ____
    - FAP ____

8. Impact on Victim
    - Helplessness _____
    - Anxious _____
    - Anger _____
    - Other Explain:_____

9. Document patterned behavior of Subject (Make sure this is documented in the ROI and/or Victim stmt)

10. Interview witnesses
    - Family ____
    - Friends ____
    - Neighbors _____
    - Co-workers ____
    - Others _____

11. Compile a contingency plan
    - List of safe places

      _____
      _____
      _____
      _____
      _____

    - Full tank of gas _____
    - Critical telephone numbers

      _____
      _____
      _____
      _____
      _____
      _____
      _____

Subject Interview Protocol

1. Identify Objectives of the Subject
- Behavior of the Subject? (Expand as needed)
- State of mind while talking to the subject?
- Other possible targets?

2. Construct detailed information pertaining to all alleged offenses
- Time of incident(s)
- Place of incident(s)
- Context (circumstances of each incident)

3. Focus on specifics when interviewing

4. Emphasize subject sensitivity.

5. Allow subject to tell their side of the story

6. Remain subject centered rather than penal code centered

7. Maintain focus and pace of the interview through documentation
- "Wait a moment, I need to get this down"
- "What you're saying is important"
- "Please repeat that, it is important to you, and I want to be able to understand what you are saying."

8. Provide an opportunity for further disclosure
- Additional information relaying details or other targets
- Perhaps they don't fully understand based on what has been communicated
- Are there additional details that we have not discussed that might effect how others perceive the situation

9. Document non-verbal's
- Nervous
- Anxious
- Other actions

10. Compile an action plan

Review with subject what he can anticipate in terms of law enforcement response should communication/actions continue
- Incarceration
- Enhanced bail

11. Document obsessions that subject may have
- Photographs
- Videos
- Journals

CHAPTER 4
TITLE: GENERAL CRIMINAL PROCEDURE
POC: CODE 00L
DATE: SEP 07

4-1. GENERAL

Before being put on trial, a suspected criminal must be brought before the tribunal having jurisdiction over the subject matter and the accused. In civilian life, this is accomplished usually by the arrest of the suspect. In military life, however, in the majority of cases, the offender is already within military control and ensuring availability for trial can usually be accomplished by the imposition of appropriate administrative measures. When, on occasion, it becomes necessary to take into physical custody a person subject to the Uniform Code of Military Justice (UCMJ), authority is provided under the UCMJ and the Manual for Court-Martial (Manual of the Judge Advocate General (JAGMAN), section 0117). A discussion of the authority and procedures relating to apprehension of persons by NCIS agents is contained in NCIS-3 Chapter 16.

4-2. ACQUISITION OF EVIDENCE

The procedural consequences that flow from the unlawful acquisition of evidence through a violation of the 4th and 5th Amendments to the U.S. Constitution and Article 31 of the UCMJ are substantial. Courts will exclude evidence acquired in violation of Constitutional and statutory protections. Some instances in which evidence will be so excluded are those in which it was obtained 1) through illegal search and seizure; 2) in violation of the right of the accused to freedom from compulsory self-incrimination; or 3) through unlawful interception of a telephone conversation. The rules in this area are of the utmost importance to the criminal investigator. NCIS agents should be aware that courts-martial also follow the exclusionary rules with regard to these matters.

4-3. PRELIMINARY HEARING

4-3.1. A person who has been arrested or placed in confinement cannot be held in custody indefinitely without further proceedings. In civilian cases, the person making the arrest, or the person to whom the arrested person is delivered, must see to it that the arrested person is taken "as soon as possible" or "immediately" before the nearest or most accessible magistrate or other person authorized to admit to bail and hold preliminary hearings. Failure to do so may result in liability for false imprisonment. **NOTE**: The parallel requirement in military procedure is that a person being apprehended must be taken promptly before his/her Commanding Officer or other appropriate military authority. Agents may be asked to transport the apprehended person to the nearest brig.

4-3.2 In the military, before a charge or specification can be referred to trial by general court-martial, a thorough and impartial investigation pursuant to Article 32, UCMJ must be conducted. The Article 32 investigation includes an inquiry as to the truth of the matter set forth in the charges, consideration of the form of charges, and a recommendation as to the disposition of the case in the interest of justice and discipline. An Article 32 investigation is not required for charges referred to a special court-martial.

4-4. STATUTE OF LIMITATIONS

The time within which indictments may issue or proceedings commence for crimes and offenses varies considerably between jurisdictions, and generally depends upon the gravity of the offense. For example, under the UCMJ a person charged with absence without leave in time of war or with any offense punishable by death may be tried and punished at any time without limitation (Article 43, UCMJ). The statute of limitations for prosecution for most offenses, except as otherwise provided for by Article 43, is five years from the time of the offense until the receipt of sworn charges by an officer exercising summary court-martial jurisdiction over the command.

4-5. GRANTS OF IMMUNITY

4-5.1. The ends of justice are sometimes served by offering grants of immunity to prospective witnesses who might otherwise invoke the privilege against self-incrimination. There are two types of grants of immunity: testimonial or use immunity and transactional immunity. When a witness is granted testimonial immunity, the government may not subsequently use his/her testimony, or evidence derived from it, in a prosecution against him/her. A testimonial grant is not, however, a bar to prosecution based upon independent evidence. Transactional immunity is broader. A witness who testifies under a transactional grant of immunity may not be prosecuted for any transaction, i.e., act or offense about which he/she testifies, even if the government obtains independent evidence of his/her criminal involvement. Traditionally, grants of immunity in the military have been testimonial.

4-5.2. A prospective military witness may not reject a grant of immunity. Failure to testify after a grant of immunity has been made is punishable as a violation of Article 92, UCMJ. A grant of immunity for a military witness in a trial by court-martial, where the charges do not involve matters of espionage, national security or classified documents/information, may only be given by an officer exercising general court-martial jurisdiction (OEGCMJ). Immunity for civilian witnesses at courts-martial must be forwarded by the OEGCMJ to the JAG, who will attempt to obtain approval for the grant from the Attorney General. All requests must be made in writing and contain sufficient information to make an informed decision, i.e. background information regarding the investigation, reasons for the request, and anticipated testimony of the witness. The JAGMAN, Sections 0138 and 0139, provides additional guidance regarding requests for grants of immunity for civilian testimony in trial by courts-martial.

4-5.3. The U.S. Attorney, with the approval of the Attorney General or designee, may grant immunity to a witness in federal court or federal grand jury proceeding when:

a. The testimony or other information from the person may be necessary to the public interest and

b. The individual has refused or is likely to refuse to testify or provide other information on the basis of his/her privilege against self-incrimination.

4-5.4. NCIS personnel must ensure that they do not cause a prospective witness to believe that NCIS can grant or directly obtain a grant of immunity. If a prospective witness solicits information about a grant of immunity, he/she should be informed that his/her interest will be made known to the proper military or civilian authority. The matter should then be referred to the Staff Judge Advocate, the Trial Counsel, or the appropriate U.S. Attorney.

4-5.5. In unusual circumstances, subject to prior approval of the parent NCISFO, it may be appropriate for the investigating special agent or NCISRA to recommend to the OEGCMJ or appropriate U.S. Attorney that a grant of immunity be extended to a particular prospective military or civilian witness. For example, this procedure might be appropriate in a case where the testimony of one principal may be needed to convict the other principals in an offense.

4-5.6. Grants of Immunity in Cases Involving National Security. In all cases involving national security or foreign relations, the cognizant OEGCMJ shall forward, in prescribed form, any prepared grant of immunity to JAG (via OJAG Code 17) for the purpose of consultation with DOJ. See JAGMAN 0138.

4-5.7. Other Requirements. After a military or civilian grant of immunity has been approved and obtained, the interview of the suspect should be coordinated with the suspect's attorney, if any. A self-incrimination warning should be provided and the terms of the grant should be explained to the suspect before the interview begins; the limits of the grant should also be set forth in any written statement obtained from the suspect. If the suspect provides incriminating information regarding offenses not covered by the grant of immunity and the special agent wants to follow-up with questions regarding those admissions or confessions, the special agent should provide warnings against compulsory self-incrimination in accordance with Article 31(b), UCMJ.

4-6. JURISDICTION

4-6.1. NCIS has global authority to investigate violations of the punitive articles of the UCMJ committed by members of the naval service and criminal violations of the U.S. Code by members of the naval service or employees of the Department of the Navy (DON), and to investigate if the DON is the victim of a crime. NCIS may also conduct other investigations as requested by higher authority.

4-6.2. Assimilative Crimes Act. By this statute, Congress provided that all acts or omissions occurring in an area under Federal jurisdiction, that would constitute crimes if the area were under state jurisdiction, constitute the same crimes, similarly punishable, under Federal law. For illustration, Congress has not enacted a traffic code; however, a person speeding on a naval base could be charged with a Federal violation because the local state's traffic laws (if speeding is a criminal offense in the state) are adopted for Federal use on the base. The Assimilative Crimes Act is found at 18 USC 13.

4-6.3. Territorial Jurisdiction. Military reservations are generally categorized as having either exclusive Federal jurisdiction or concurrent federal jurisdiction. The Federal government may also hold territory in a status of proprietorial interest. There are a number of bases, however, that are not solely one type of jurisdiction or the other but are instead a mixture. Because parts of the base were acquired at different times in different ways, one portion might be exclusive jurisdiction and the next concurrent. Agents should consult with their local public works or Staff Judge Advocate as to the jurisdictional status of all portions of their base. See, also, 18 USC 7.

a. Exclusive Jurisdiction. Only the Federal government has the power to make and, through its various agencies including the military, enforce the law in areas of exclusive Federal jurisdiction. Thus, only the specific Federal criminal statutes and the crimes adopted through the Assimilative Crimes Act are applicable. State laws have neither direct force nor effect and local, state, or municipal law enforcement authorities have no authority on such land.

b. Concurrent Jurisdiction. Both the Federal government and state government, including its county and municipal subdivisions, have authority to make and enforce laws on the land in question. Thus, one offense could be a crime under both federal and state or local law. Both naval authorities and state authorities could enforce and prosecute their respective laws.

c. Proprietorial Interest. When the Federal government has acquired title to a piece of property but has not obtained legislative authority over the area, only the state generally has the power to enforce its law on the property. The U.S. has the right, however, as does any landowner, to protect its property. In addition, state authorities cannot interfere with any valid military activity on such property.

4-6.4. NCIS agents should be aware of the following limitations on prosecutions under the UCMJ.

a. UCMJ. Art. 2 indicates that, in time of war, persons serving with or accompanying an armed force in the field are subject to the UCMJ. The definition of “time of war” was recently expanded to include “contingency operations” such as our current operations in Iraq and Afghanistan.

b. The advice of counsel should be obtained if the investigation focuses upon a suspect recently released from active duty or recently re-enlisted.

4-6.5. Military Extraterritorial Jurisdiction Act of 2000 (MEJA). MEJA is a Federal statute, 18 USC 3261-67, that provides a mechanism for closing a jurisdictional gap in U.S. law to permit the criminal prosecution of covered persons for offenses committed outside the United States. Covered persons include: civilians employed by or accompanying (including dependents) the Armed Forces outside the United States and former members of the Armed Forces who committed offenses punishable by more than 1 year imprisonment while serving as a member of the Armed Forces outside the United States. Department of Defense Instruction 5525.11, Criminal Jurisdiction Over Civilians Employed By or Accompanying the Armed Forces Outside the United States, Certain Service Members, and Former Service Members (2005), is the governing instruction that implements MEJA in the Armed Forces.

NCIS-3, Chapter 5
Evidence
Effective Date: August 2013

Table of Contents:

References:

(a) Manual for Courts-Martial (MCM), United States (2012 Edition)
(b) DoD 6025.18-R DoD Health Information Privacy Regulation, January 2003
(c) NCIS-3, Chapter 17, Search and Seizure
(d) NCIS-3, Chapter 36, Electronic Interceptions and Electronic Investigative Aids
(e) NCIS-3, Chapter 6, Investigative Theory and Procedures
(f) NCIS-6, Chapter 13, Evidence Custody System
(g) NCIS- 1, Chapter 21, Personal Privacy Act
(h) NCIS-3, Chapter 7, Rights, Warnings, and Self-Incrimination

5-1. Purpose. This chapter provides an overview of evidentiary rules and limitations applicable to military criminal investigations. Information contained in this chapter is based on references (a) and (b). Provisions of this chapter apply to all personnel involved in handling, gathering and reviewing evidence. Awareness of evidentiary rules increases the effectiveness of investigations in supporting successful prosecutions and maintaining good order and discipline within the Navy and Marine Corps.

5-2. Policy. All personnel involved in criminal investigations shall be familiar with the rules of evidence.

5-3. Cancellation. NCIS-3, Chapter 5, dated October 2007.

5-4. Chapter Sponsor. Counsel to the Director, Code 00L.

5-5. Sources of Rules. Rules of evidence for courts-martial derive from: the United States Constitution, the Uniform Code of Military Justice (UCMJ), the Manual for Courts-Martial (MCM) including the Military Rules of Evidence (Mil. R. Evd.) and Rules for Courts-Martial (R.C.M.), the decisions of the U.S. Supreme Court, the Court of Appeals for the Armed Forces, the Navy-Marine Corps Court of Criminal Appeals, and rulings of military judges at trial. Sources of evidentiary rules that may be persuasive but are not binding include: other provisions of the United States Code, the Federal Rules of Evidence, other federal court opinions, state court opinions, and legal writings.

5-6. Classifications of Evidence. Evidence is testimony and material presented to a fact-finder (jury or judge in a bench trial). Evidence is not fact. Instead, it helps fact-finders determine if facts are proved to a particular standard (generally beyond a reasonable doubt for criminal court proceedings). No particular category of evidence trumps other types.

a. Testimonial evidence is presented in the form of spoken words. The witness to a crime verbally relates what they saw, heard, smelled, touched, or tasted concerning that crime. Examples include what was seen and heard in the course of witnessing a fight or what was seen and smelled while witnessing someone using marijuana.

b. Evidence may also be in the form of real evidence and other material objects. Real evidence may be contrasted with testimony, and includes physical items such as guns, photographs, clothing, or drugs seized. Documentary evidence consists of papers such as travel claims, written contracts, letters, e-mails, web pages, etc. Objects may be admitted into evidence once a foundation is laid, giving background and explanation of their significance. Documentation establishing fingerprints belonging to a particular person on a glass at the scene provides evidence the person may have been in the room. Tool marks on a lock at the scene of a break-in provides evidence that a certain tool was used.

c. Demonstrative devices may also be introduced to illustrate and summarize evidence. Examples include crime scene sketches, diagrams, and models.

5-7. Uses of Evidence. Evidence may be used to prove facts in either of two ways (1) directly or (2) circumstantially (as defined in R.C.M. 918):

a. Direct evidence simply points to a fact at issue (element of the crime). Example: a witness says that he/she saw the accused rob the victim. This testimony points directly to the accused as the person who committed the crime.

b. Circumstantial evidence is introduced to prove other facts or circumstances from which one can infer a fact at issue. Example: given a room with one person in it and only one opening, someone walks in with a gun, shots are heard, and the person walks out; no one else comes or goes from the room; and the person who was originally in the room is found dead of gunshot wounds. Assuming that suicide, self-defense, or accident can be ruled out, it can be logically inferred that the

person with the gun committed a murder. The evidence shows facts, each of which may be harmless in itself; but the inferences that may be drawn from those facts, indicate a murder, even though no one directly saw the crime take place.

5-8. Admissibility. To be admitted, evidence must be competent, authentic, relevant, and not subject to any privilege, exclusionary rule, or other legal objection. The fact-finder will only consider evidence admitted by the judge.

a. Competence. This standard applies both to evidence and witnesses.

(1) As applied to evidence, competence means that the evidence has been obtained in such a way and form, and from such a source that it is deemed proper to admit it. Evidence that the defendant shot the victim is relevant in a prosecution for the victim's murder, but the evidence would be incompetent if offered by a person whose only knowledge of the defendant is what the person heard from people in the neighborhood.

(2) As applied to a witness, competence means that a degree of maturity and mental capacity that will justify admitting that person's statement into evidence. A confession may be very relevant to a case on trial and clearly be shown to be the defendant's, but it will be incompetent as evidence if it was improperly obtained.

b. Authenticity. The test for authenticity is whether the evidence being presented is really what it purports to be. Testimonial evidence is authenticated by an oath or affirmation. If a document is being offered into evidence, unless it is self-authenticating, someone must establish that it actually is the document that it is represented to be. The document custodian may do this by taking the witness stand and saying they recognize the document, it bears their signature, or it came from their files. If the prosecution seeks to show that the baseball bat in court is the same one used to beat a victim, a person who took it from the accused's hands could testify to those facts. Evidence may also be authenticated by seals or attesting certificates. An official confirms drug lab analysis result documents by attesting certificates to the fact that the documents are a laboratory analysis.

c. Relevance. Mil. R. Evd. 401 defines relevant evidence as: “evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence.” The key question could be restated as whether the evidence aids the court in answering the question before it. If the answer to that question is yes, then the evidence sought to be introduced is probably relevant. If not, it is subject to proper objection by the other side. However, even if evidence is relevant, it may still be excluded if the judge feels that it is prejudicial beyond its usefulness to the trier of fact, confusing, or simply a waste of time to present.

5-9. Exclusionary Rule. Courts will exclude evidence acquired in violation of Constitutional and statutory protections, in particular the 4th and 5th Amendments to the U.S. Constitution and Article 31 of the UCMJ. Some instances in which evidence will be so excluded are those in which it was obtained: (1) through illegal search and seizure; (2) in violation of the right of the accused to freedom from compulsory self-incrimination; or (3) through unlawful interception of a telephone conversation. The exclusionary rule is designed to deter unlawful police conduct by excluding the

results of such conduct from use in a trial. Derivative evidence obtained during subsequent investigative activities may also be excluded, as "fruit of the poisonous tree." Mil. R. Evd. 311 provides additional detail on the exclusionary rule, its exceptions, and procedures (motions and objections).

5-10. Privileges. Privileges are excusals from the general requirement to testify and produce evidence. There are a number of privileges available at criminal trials; some are applicable in the military and found in Mil. R. Evd. Sections III and V. The following are some of the more common privileges likely to be encountered:

a. Compulsory Self-Incrimination. Mil. R. Evd. 301 derives from the Fifth Amendment of the United States Constitution and Article 31 of the UCMJ. Individuals may refuse to respond to questions or produce evidence that may tend to incriminate them. The privilege may be exercised or waived at the discretion of the individual but may be negated through the use of a grant of immunity or the running of the statute of limitations.

b. Statements During Mental Examination. This privilege arises under Mil. R. Evd. 302 when an accused sees a psychiatrist not for diagnosis or treatment, but rather to determine his/her mental responsibility for alleged criminality (under R.C.M. 706). Whether or not an accused has been given appropriate warnings, he/she has a privilege to exclude such evidence on the merits or during sentencing. The privilege is dissolved if the individual first introduces the statements or derivative evidence.

c. Psychotherapist-Patient Privilege. Some civilian jurisdictions grant a broad privilege for confidences between doctors and patients. Mil. R. Evd 513 limits this to psychotherapists, clinical social workers and their assistants. The privilege only exists for the life of the patient and has several exceptions, including for domestic violence, child neglect, and patients who pose a danger to themselves or others. Medical treatment unrelated to mental health is not privileged, but see section 5-15(b) below for discussion of privacy and medical records.

d. Victim Advocate-Victim Privilege. Mil. R. Evd 514 grants this privilege to victims of sexual or violent offenses for confidential communications made to designated or authorized victim advocates for the purpose of facilitating advice or supportive assistance to the victim. Limitations are similar to those for the psychotherapist-patient privilege above.

e. Attorney-Client Privilege. Mil. R. Evd 502 grants clients a privilege over confidential communications made between clients and attorneys (and their representatives) for the purpose of providing legal services. This privilege does not apply when the communications are made in clear contemplation of the future commission of a crime, fraud, or client malpractice allegations against the attorney.

f. Communications to Clergy. Mil. R. Evd 503 states "a person has a privilege to refuse to disclose and to prevent another from disclosing a confidential communication by the person to a clergyman or to a clergyman's assistant, if such communication is made either as a formal act of religion or as a matter of conscience." A clergyman includes a minister, priest, rabbi, chaplain, other similar functionary of a religious organization, or an individual reasonably believed to be so

by the person consulting the clergyman.

g. Husband-Wife Privileges. Mil. R. Evd 504 provides privileges listed below which are both dissolved in cases where one spouse is charged with a crime against the person or property of the other spouse, a child of either, or a third person committed in the course of committing a crime against the other spouse. Exceptions also apply for sham marriages and allegations involving importing or transporting ones' spouse in interstate commerce for immoral purposes. The two husband-wife privileges are:

(1) Testimonial (spousal incapacity). A person can refuse to testify against his/her current spouse.

(2) Communications. Either spouse can assert privilege over confidential communications made within marriage. Unlike the testimonial privilege, this survives a broken marriage.

h. Protection of Information. Mil. R. Evd 505 provides that classified information is privileged from disclosure if disclosure would be detrimental to national security. Mil. R. Evd 506 allows the government to claim privilege for unclassified information if disclosure would be detrimental to the public interest, such as where public knowledge of NCIS' techniques could harm future investigations. Neither rule is absolute; an accused's constitutional rights may necessitate at least partial disclosure or dismissal of charges.

i. Identity of Informant. See section 5-16 below for more detail on Mil. R. Evd 507. When an informant provides only probable cause as to search or seizure or an arrest and is not a witness as to guilt or innocence of an accused, it is possible to protect the identity of the informant.

j. Deliberations. The deliberations of judges, trial juries, and grand juries and political votes are privileged under Mil. R. Evd 508 and 509.

5-11. Lay and Expert Opinion Evidence

a. Lay witnesses are usually called to present factual observations. They may provide limited opinions under Mil. R. Evd 701, where the opinions are not based on scientific, technical, or specialized knowledge.

b. Experts are generally called to testify for their reasoned opinions. They may qualify as experts under Mil. R. Evd 702 based on knowledge, skill, experience, training, or education, and may generally testify as experts if their scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or determine a fact in issue. Case agents should generally not testify as experts on NCIS policy or scientific matters. Instead, special agents should refer such expert requests (and prosecutors) to Code 00L for assistance as soon as possible.

5-12. Evidence of Other Crimes or Misconduct

a. Special agents may uncover additional misconduct on the part of a suspect or witness that is not directly related to the case on trial. The rules of evidence place limits on when and how other

convictions or misconduct may be received into evidence simply because of the distracting nature of such misconduct from the case on trial. In limited circumstances, evidence of prior misconduct of the accused or witness testifying may be received into evidence in order to impeach the testimony by attacking the character of the accused or witness.

b. Impeachment. The act of discrediting a person or a thing by showing a prior inconsistent statement, an inability of the witness to perceive what that witness just testified about, or by showing bias and prejudice or corruption on the part of the witness. Witnesses may also be impeached by opinion or reputation evidence referring to their character for untruthfulness. In certain limited circumstances evidence can be introduced showing previous crime convictions to discredit the integrity of a witness. When the accused becomes a witness, they become subject to impeachment just like any other witness.

5-13. Hearsay. Hearsay is a statement, made out of court, offered to prove the truth of the matter asserted. Some admissions and prior testimony subject to cross-examination are not considered hearsay as defined by Mil. R. Evd 801. Hearsay is generally inadmissible, but there are numerous exceptions allowing evidence under Mil. R. Evd 803 through 807.

a. Present Sense Impression. A statement describing an event or condition made while the declarant perceives the event, condition or immediately thereafter.

b. Excited Utterance. A statement relating to a startling event or condition made while the declarant was under the stress of excitement caused by the event or condition.

c. A statement of the declarant's then existing state of mind, emotion, sensation, or physical condition (such as intent, plan, motive, design, mental feeling, pain, and bodily health).

d. Statements for purposes of medical diagnosis or treatment.

e. Recorded Recollection. A memorandum or record (such as agent notes) concerning a matter about which a witness once had knowledge but now has insufficient recollection from which to testify accurately. The witness must show the writing, which is read into evidence, was made when their memory was fresh and accurate.

f. Records of Regularly Conducted Activity ("Business" Records). Note that the exception for business records requires that evidence be kept in the course of a regularly conducted business activity, that recording the information was the regular practice of that business activity, and the record was made at or near the time or event by a person with knowledge. Government and Armed Forces records may be introduced under this hearsay exception. Evidence of an absence of records or entries may also be introduced. Laboratory reports, service records, and chain of custody documents are generally admissible under this rule. Law enforcement reports are not.

g. Other hearsay exceptions include: (1) public records and reports; (2) records of vital statistics; (3) absence of public record or entry; (4) religious, marriage, and family records; (5) records and statements in documents affecting an interest in property; (6) statements in ancient documents; (7) market reports and commercial publications; (8) learned treatises; (9) reputation concerning

personal or family history; (10) reputation concerning property boundaries or general history; (11) reputation as to character; (12) judgment of a previous conviction; (13) judgment as to personal, family, or general history, or boundaries; (14) former testimony; (15) statement under belief of impending death; (16) statement made against the financial, criminal, or other interest of the speaker; and (17) any matter having circumstances guaranteeing trustworthiness.

5-14. Searches and Seizures

a. The military law of search and seizure is partially codified in Mil. R. Evd ... 311 to 316. See reference (c) for more information.

b. Oral, Wire, and Electronic Interceptions. See reference (d) and Mil. R. Evd 317 for more information.

5-15. Financial and Medical Records

a. Financial Records. The evidentiary requirements involved in the obtaining of financial records are discussed in references (e) and (f).

b. Medical Records. The Health Insurance Portability and Accountability Act (HIPAA) was implemented within DoD by reference (b) which is the controlling instruction for NCIS and addresses requests for protected health information (PHI) from covered entities such as military treatment facilities (MTF). HIPAA is more restrictive than the well-known Privacy Act, covered by reference (g). In many instances, the Privacy Act permits the release of such records to those individuals within DoD who have a legitimate need to know; HIPAA and reference (b) do not. In the case of NCIS requests for PHI, the following applies:

(1) Armed Forces Personnel. PHI is not releasable under HIPAA unless an exception exists. If an exception permits release, only the minimum necessary information may be released unless a general record release is otherwise specifically permitted by the exception. MTF release of PHI to NCIS and commanding officers is permitted based on either the "military mission" or "delegated official" exception and not the "law enforcement" exception, which, for purposes of reference (b), generally pertains to requests from civilian law enforcement entities. An MTF may release PHI on Armed Forces personnel directly to an NCIS agent upon receipt of a proper written request; however, the minimum necessary rule does apply. This requires the requesting agent to specify the need for, and scope of, the information requested, and the MTF to ensure that the content of the records released is limited to that specific need and scope. NCIS cannot disclose health records outside DoD. Case agents should summarize relevant information in an investigative action and advise other interested law enforcement agencies that they can submit their own requests to MTF's under paragraph C7.6.1.2.3 of reference (b).

(2) Civilian Personnel. MTFs in some circumstances (e.g., medical records of minors) may require a signed release or court order before providing PHI to NCIS.

5-16. Disclosure of Informant Identity. (Identity of informants, under Mil. R. Evd 507)

a. Unless otherwise privileged under the rules of evidence, the communications of an informant

are not privileged except to the extent necessary to prevent the disclosure of his/her identity. The privilege may be claimed by an appropriate representative of the U.S. or a particular state regardless of whether the information was furnished to an officer of the U.S. or of a state or subdivision thereof.

b. This privilege no longer applies if there is voluntary disclosure, such as where an informant testifies as a witness. Likewise, a judge may determine that disclosure is necessary to the accused's defense on the issue of guilt or innocence, or that an accused has a constitutional right to disclosure, such as where there is a question of whether search and seizure was properly founded.

c. If a court determines that disclosure is required, and the prosecution elects not to disclose the identity of the informant, the matter shall be reported to the convening authority. The convening authority may institute action to secure disclosure of the identity of the informant (such as immunity), terminate the proceedings, or take such other appropriate action under the circumstances.

5-17. Self-Incrimination. The evidentiary aspects of self-incrimination are covered in reference (h).

(b)(7)(E)

5-19. Disclaimer. The NCIS-3 manual, including this chapter, is set forth solely for the purpose of internal agency guidance. The manual is not intended to, does not, and may not be relied upon to create any rights, substantive or procedural, enforceable at law by any party in any matter, civil or criminal, and it does not place any limitations on otherwise lawful activities of the agency.

CHAPTER 6
TITLE: INVESTIGATIVE THEORY AND PROCEDURES
POC: Code 23C
DATE: DEC 06

APPENDICES:

POLICY DOCUMENTS

APPENDIX (3) Gen Admin 11-0027 of 26 July 2011 released NCIS Policy Document No. 11-15 Operational (Submitting Fingerprints To Query The FBI's Integrated Automated Fingerprint Identification System (IAFIS). Policy document 11-15 contains revised or new policy that has been incorporated into this chapter and should be reviewed in its entirety.

APPENDIX (4) Gen Admin 11C-0032 of 6 September 2011 released NCIS Policy Document No. 11-18 Operational (Using the Electronic Military Personnel Records System). Policy document 11-18 contains revised or new policy that has been incorporated into this chapter and should be reviewed in its entirety.

APPENDIX (5) Gen Admin 11C-0034 of 30 September 2011 released NCIS Policy Document No. 11-19 Operational (Submitting Fingerprints To Enroll Into the FBI's Integrated Automated Fingerprints Identification System (IAFIS)). Policy document 11-19 contains revised or new policy that has been incorporated into this chapter and should be reviewed in its entirety.

APPENDIX (6) Gen Admin 11C-0003 of 6 February 2012 released NCIS Policy Document No. 12-02 Operational (Deoxyribonucleic Acid (DNA) Collection Requirements for Criminal Investigations). Policy document 12-02 contains revised or new policy that has been incorporated into this chapter and should be reviewed in its entirety.

APPENDIX (7) GEN Admin 11C-0001 of 3 January 2013 released NCIS Policy Document No. 13-01 Operational (Financial crimes Enforcement Network Support and Bank Secrecy Act Information). Policy document 13-01 contains revised or new policy that has been incorporated into this chapter and should be reviewed in its entirety.

APPENDIX (8) GEN Admin 11C-0006 of 21 February 2013 released NCIS Policy document No. 13-03 Administrative (Establishment Of The Reserve Master-At-Arms Program). Policy Document 13-03 contains revised or new policy that has been incorporated into this chapter and should be reviewed in its entirety.

6-1. DEFINITION

6-1.1. An investigation is a detailed, objective inquiry to ascertain the truth about an event, situation or individual. It is comprised of four phases: Analysis, Programming, Fact Finding, Verification and Evaluation. The degree to which each phase plays a part in any given investigation differs according to the circumstances of that investigation. It is important to know that each phase plays some part in each investigation and to consider each phase during the conduct of an investigation.

a. Analysis. At the beginning of any NCIS investigation an agent must analyze the complaint; analyze the complainant, and analyze the jurisdiction. The analysis phase determines: whether the complaint has merit; whether the matter to be investigated falls within the investigative jurisdiction of the NCIS; and whether the complainant is providing valid information regardless of motives. Not infrequently, a preliminary investigation is conducted to determine if a crime exists and to identify likely suspects. Based upon the preliminary investigation, the jurisdictional aspect of the analysis phase can be resolved.

b. Programming. Once the analysis phase of an investigation has been completed, it is time to program or outline the investigative steps to be followed in order to elicit information and where appropriate to develop proof of all essential elements of an alleged violation or offense. A logical preliminary outline should include the essential elements of an indicated offense, as prescribed by pertinent law or regulation, etc., with additional topics to cover informative phases of the investigation. In preparing and developing the outline, consideration should be given to the evidence required and the possible sources of information and evidence. It is not intended that the outline should be formal and inflexible in scope. In less complicated cases involving matters, which occur repeatedly, this process may be a simple mental exercise that takes only minutes of an Agent's time. In more complex investigative matters, it would be wise to reduce this process to written form and to review the programming during the course of the investigation, retaining a flexible approach that permits reconsideration as the circumstances of the case require. Programming is essentially a process employed by a professional investigator as an intelligent approach to an investigation that ensures that all essential elements are addressed and that all unnecessary aspects are avoided. The manner in which the outline is prepared and its extent are discretionary.

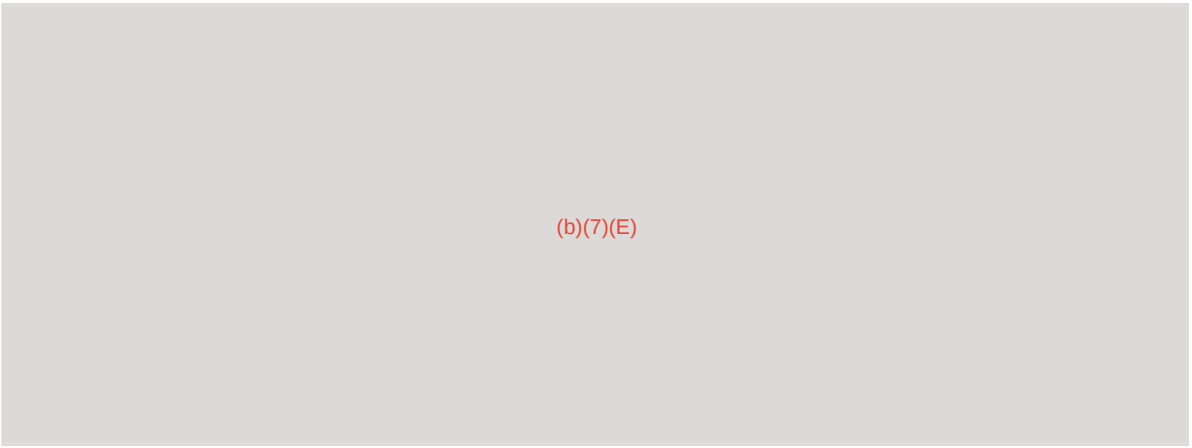
c. Fact-Finding. To establish the existence or nonexistence of the elements outlined through observing; interviewing complainants, witnesses and subjects; examining records and documents; and securing testimony of witnesses and documentary and physical evidence. This fact-finding phase also includes full inquiry into any exculpatory or alibi information. As facts and information are gathered, the programming will evolve more fully, tangents will be avoided, and the investigation will develop evidence consistent with the involvement of the subject under investigation.

d. Verification and Evaluation. To establish the accuracy and authenticity of testimony, records, and other documentary and physical evidence. Throughout the investigation, information obtained should be checked against the outline or programming. Conflicting testimony or information as to material matters must be resolved by obtaining additional evidence from other competent witnesses and sources. In evaluating testimony of witnesses, one should be cognizant of the witness' interest, bias, prejudice, integrity, reputation, sense deficiencies, and also, the manner in which the information was acquired. This last phase becomes important when a case goes to court and a defense lawyer, who is assisted in his/her efforts by the cooperation of the accused, challenges the evidence developed during the course of the investigation. The more verification that can be obtained for each essential element of the offense, the less likely that element can be successfully challenged in court.

6-2. COMPLAINT AND APPROACH TO INVESTIGATION

(b)(7)(E)

Pages 70 through 71 redacted for the following reasons:
- -
(b)(7)(E)



6-3. RECORDS INFORMATION

6-3.1. Records Information is defined as any record, custodian of records, directory, public or business official, or similar source of recorded data, which may furnish assistance in the conduct of an investigation. Records Information is best thought of as being of an official or quasi-official nature, distinguished from private individual (cooperating witnesses) sources such as acquaintances, co-workers, neighbors and various other developed personal contacts unique to a particular individual/suspect or investigation/operation.

6-3.2. This section is intended to serve the NCIS Representative as a basic guide to acquire the needed information and/or to stimulate thinking and exploration as to where the required information may be obtained. The changing nature and titles of record sources occasionally makes previous sources obsolete. Thus, the list should be considered a potential reference as to certain kinds of record information that can be obtained. Restrictions on access to information resulting from a record source's policy, particularly as imposed by the Freedom of Information and Privacy Acts, necessitate emphasizing that the list only identifies the probable existence of informational holdings. The availability of data will frequently require certification of a legitimate need for the information; information made available to NCIS will often result in the record source immediately or eventually apprising the individual (Subject) of the fact that information concerning him/her was released to NCIS. A NCIS Representative cannot force a person/official to divulge information or compel another to make records in his/her possession available, nor always preclude the subject of the information from learning of the divulgence. (Note NCIS-1 Chapter 21, Section 2105.1.c, regarding the Privacy Act in this respect.) Certain Federal and Department of Defense records can be obtained by NCIS through solicitation to appropriate authority, however; only a subpoena or court of competent jurisdiction can compel divulgence from civilian sources. Coordination with Code 23 CI, Criminal Intelligence Division, is recommended.

6-3.3. Following is a list, and in some cases a brief description, of sources of official recorded information most frequently consulted by NCIS:

a. Federal Records

(1) Department of the Navy.

(a) Information pertaining to ship movements is best obtained from those NCIS offices servicing the homeports of the ships in question. A list of ship homeports can be viewed at the U. S. Navy's web site. The homeport list by ship name is located at: http://www.chinfo.navy.mil/navpalib/ships/lists/shipalfa.html

(b) Department of Defense Employee Interactive Data System (DEIDS) can serve as a military personnel locator file for all branches of the military. For those offices without direct access to DEIDS, military personnel locator files can be accessed through the Criminal Intelligence Unit (CIU), Code 0023CI. Navy and Marine Corps personnel locator files can also be requested by contacting the NCIS Multiple Threat Alert Center (MTAC). DEIDS can also be used to locate military family members and DOD civilian employees in the GS, WG, and SES series.

(c) The best source of specific information concerning a service member is that member's local service record. Navy service records are either Enlisted Service Records (ESRs) or Officer Qualification Records (OQRs). Marine Corps service records are Service Record Books (SRBs). Service records of personnel assigned to deployable units are normally filed in the Personnel Office or Administrative Office of the unit. Service records of shore-based personnel are normally on file at the servicing Personnel Support Detachment (PSD). In rare instances in which, for reasons of operational security, it is not feasible for NCIS personnel to review locally available service records, the permanent records on file at either Navy Military Personnel Command (NMPC) Millington, TN or Headquarters Marine Corps Quantico, VA can be reviewed. Permanent service records are not as complete as the locally available service records. Reviews of permanent service records will require leads to be sent to NCISRA Memphis, TN or NCISRA Quantico, VA as appropriate.

(2) Defense Central Index of Investigations (DCII). Through the DCII, NCISHQ has an almost instantaneous computerized capability of determining whether a particular subject has an existing investigative dossier on file within the Department of Defense (DOD). In addition to NCIS, contributors to the DCII are the U.S. Army Investigative Repository (AIRR), U.S. Army Crime Records Directorate (ACRD), the Air Force Office of Special Investigations (AFOSI), the Defense Criminal Investigative Service (DCIS), and the Defense Security Service (DSS). Upon determining the existence and whereabouts of a dossier, NCISHQ can normally obtain pertinent contents on a priority basis. DCII data identifies individuals investigated by names, date of birth, Social Security Number (SSN), place of birth, and service dossier number. To increase the success of getting a "hit" from a DCII inquiry, an individual's name with a date or place of birth or SSN is needed. Without a name, a SSN is needed.

(3) Defense Security Service (DSS)/Other Military Services. In addition to the DCII resource cited above, through established liaison with DSS and other counterpart service agencies (Army's Assistant Chief of Staff for Intelligence (ACSI) and Criminal Investigation Command, AFOSI, USCG Intelligence, and the Director of Intelligence,

USMC), NCISHQ can readily obtain personnel and unit locator information, as well as specific and centrally available information unique to those services.

(4) Department of Justice

(a) Federal Bureau of Investigation. Both at the field level and at the seat-of-government, the FBI provides NCIS with access to the central (Federal) repository of investigative files, as well as to FBI "rap sheets" which reflect criminal offense arrests made by most other Federal, State and local agencies in the U.S. Additionally, NCIS is a member of the FBI's National Crime Information Center (NCIC), a National computerized system for readily storing and retrieving a variety of significant (i.e., lost, stolen, missing, found, wanted, etc.) criminal intelligence information contributed by Federal, State and local law enforcement organizations (including NCIS). The NCIC is accessed via NCISHQ according to procedures described in NCIS-1, Chapter 19. Additionally, most overseas NCISFOs have local access to FBI file information via the Legal Attache (LEGAT) of their respective American Embassy. FBIHQ is also a particularly important resource to the investigative community for identification of individuals/suspects through its fingerprint database.

(b) Drug Enforcement Administration. The DEA is the principal U.S. Agency concerned with narcotics and drug trafficking, both domestically and internationally. DEA is principally concerned with major international/CONUS drug trafficking matters and, by general agreement, is not concerned with investigating or receiving information relating to the typical small-time traffickers or users. DEA is a key source on drug/narcotics trafficking routes, origins and similar intelligence. In any significant drug/narcotics situations encountered by NCIS, particularly one involving U.S. civilian/foreign participants, the respective DEA field component or DEAHQ (through NCISHQ) should be consulted for pertinent intelligence, and possible referral action. (See NCIS-3 Chapter 31, Narcotics Violations.)

(5) Central Intelligence Agency. The CIA is the central repository for information on foreign intelligence matters of concern to the U.S. While most overseas NCISFOs have means of making inquiries directed to CIA holdings, NCISHQ has excellent liaison with CIAHQ to serve CONUS NCISFOs inquiries. Any queries made of CIA, via NCISHQ, should be as specific and detailed as possible in identifying individuals and the type of information/checks desired.

(6) Other Federal Agencies Frequently Contacted. NCISHQ has well-established and relatively frequent liaison with the headquarters of the following Federal investigative agencies and investigative components of non-investigative agencies, many of which have existing field office relationships with NCISFOs/NCISRAs (particularly in CONUS). A listing and brief description follows:

(a) U.S. Secret Service (USSS) (Department of Homeland Security). The USSS has responsibility for investigating any offense against the laws of the U.S.

relating to coins, obligations and securities, including counterfeiting of Federal currency and forgery of government monetary instruments. The USSS is also responsible for providing protective services to present and past Presidents, Vice-Presidents, and candidates/electrets to these offices, their families, and certain other dignitaries. USSSHQ maintains extensive indices on suspected counterfeiters, check thieves and forgers, as well as communications received, particularly those implying a threat to the President and others under their protective jurisdiction. Other government agencies, including NCIS, furnish threat communications information to both the USSS and FBI, as appropriate. It should be noted that NCISHQ retains indices on non-DOD civilians only if an implied or direct threat is made to the Department of the Navy (DON) personnel, installations or property, and subject to DIRC guidelines. (See NCIS-3 Chapters 24, 28 and 35 regarding forgery and counterfeiting offenses and protective services, respectively.)

(b) Internal Revenue Service (Treasury Department). The Intelligence Division of IRS investigates certain criminal and civil violations of Federal internal revenue tax laws except those relating to alcohol, tobacco, and firearms. By law, the IRS is considerably restricted as to what internal revenue information may be made available to the public, as well as to other Federal investigative agencies. While extremely useful information may exist in IRS records, law limits the extent to which such information may be provided.

(c) Bureau of Alcohol, Tobacco and Firearms (Justice Department). The ATF enforces Federal laws dealing with alcohol, tobacco, firearms and explosives. ATF maintains central files on individuals, partnerships and corporations issued permits to manufacture, store or trade in these items in compliance with Federal laws, as well as violations and arrest records of offenders. Investigative matters involving possible manufacturing of or trafficking in these items or certain arson matters should be discussed with the nearest ATF office.

(d) Financial Crimes Enforcement Network (FinCEN). The FinCEN is an agency under the direction of the Department of the Treasury that can provide excellent electronic database information on investigations in which the impact of financial manipulation furthers the criminal activity. FinCEN's services are especially useful on cases involving money laundering schemes, locating fugitives or witnesses, or tracking the source and destination of money. FinCEN is an intelligence organization that collects financial information from law enforcement agencies, bank regulatory agencies, credit agencies, open sources and the private sector.

(e) U.S. Immigration and Custom Enforcement (ICE) (Department of Homeland Security). ICE is charged with enforcing U.S. customs laws, supervising the importation of articles into the U.S., patrolling U.S. borders and apprehending smugglers. ICE collects information on the smuggling of merchandise, particularly concerning narcotics, marijuana, nuclear material and devices, and weapons of unconventional warfare. ICE is also concerned with the importation of prohibited or restricted articles, such as counterfeit currency and stamps, pornographic material and articles, which violate American trademarks and copyrights. (See NCIS-3 Chapter 28 regarding ICE violations.) ICE

maintains photographs, fingerprints, brief biographies, residence and employment information, circumstances of entry, and naturalization data concerning immigrants (Permanent Resident Aliens) and non-immigrants to the U.S. To aid ICE in locating an immigrant's naturalization records, the date, port of entry, and manner of arrival in the U.S. should be provided whenever possible; to check a non-immigrant's record of arrival and/or departure, full name, citizenship and date of birth should be furnished. To improve response time, ICE file checks should be made directly with the ICE field office at the port of entry or place of naturalization. ICE has advised this procedure will greatly improve response time.

(f) U.S. Coast Guard. While the USCG is now an activity of the Department of Homeland Security, its quasi-military nature and wartime relationship to the DON invite a continuing close association. NCISHQ and appropriate NCISFOs maintain excellent liaison with USCG counterparts in sharing counterintelligence information affecting the security of U.S. ports and coastlines, officers and crews of merchant marine vessels, and investigative information on USCG personnel where a common interest exists.

(g) U.S. Postal Inspection Service. Responsible for the investigation of postal violations, the Postal Inspection Service will also assist NCIS in providing mail cover information where a validated requirement exists (See Section 6-7). The Postal Inspection Service (in the United States) and Fleet Post Offices in overseas areas are essential sources for information on postal violation technicalities and regulations. (See NCIS-1 Chapter 28 regarding postal violations).

(h) Federal Records Center. The FRC at St. Louis, MO. is the central repository for personnel records (including medical records) on former military and Federal civilian personnel. Requests for personnel information from the FRC should be to NCISRU St. Louis.

(i) Department of State. In addition to security files on its own personnel, the State Department's Diplomatic Security Service has record information on many U.S. citizens and foreigners who are not State Department personnel. Additionally, the Passport Office of the Department of State is the custodian for records (applications/photographs) on U.S. passport and alien visa applicants. Queries as to whether certain information may be available from the Department of State should be directed to the appropriate NCISHQ Department.

(7) Federal Sources Infrequently Contacted. Following is an incomplete list of other Federal/seat-of-government sources, which may be able to provide record information of pertinence to a NCIS investigation/operation.

Agency for International Development (AID)
Civil Aeronautics Board (CAB)
Defense Contract Audit Agency (DCAA)
Defense Logistics Agency (DLA)
Defense Technology System Agency (DISA)

Defense Nuclear Agency (DNA)
Defense Supply Agency (DSA)
Department of Agriculture (Office of Investigations)
Department of Commerce (DOC)
Department of Energy (DOE)
Department of Health and Human Services (DHHS)
Department of Housing & Urban Development (HUD)
Department of the Interior (Division of Investigations)
Department of Labor (Wages & Hours Division)
Department of Transportation (DOT)
Federal Aviation Administration (FAA)
Federal Communications Commission (FCC)
Federal Election Commission (FEC)
Federal Emergency Management Agency (FEMA)
Federal Maritime Commission (FMC)
Federal Trade Commission (FTC)
General Services Administration (GSA)
Government Printing Office (GPO)
International Criminal Police Organization (INTERPOL)
Interstate Commerce Commission (ICC)
Law Enforcement Assistance Administration (LEAA)
Library of Congress
National Aeronautics & Space Administration (NASA)
National Institute of Health (NIH)
National Labor Relations Board (NLRB)
National Science Foundation (NSF)
National Security Agency (NSA)
Nuclear Regulatory Commission (NRC)
Office of Personnel Management (OPM)
Securities & Exchange Commission (SEC)
Small Business Administration (SBA)
Smithsonian Institution
U.S. Information Agency (USIA)
U.S. Marshal Service (USMS)
Veterans Administration (VA) (Division of Investigation)

b. State, County and Municipal Records. Sources of record information vary significantly from state to state, and between county and local governments within and between states. Unlike Federal record sources, particularly Federal investigative agencies that have a common purpose and implied relationship of mutual cooperation, state and local governmental sources have unique laws; prerogatives and attitudes which affect their ability or willingness to cooperate with Federal investigative agencies. A positive liaison effort by NCIS field components is therefore of mandatory importance to ensure that state and local sources are understanding of NCIS' mission and desire for mutual support. Following is a partial list of the types of state, county and municipal record sources which may be able to provide important investigative assistance:

(1) State:

Attorneys General Offices
Agriculture Departments
Banking Commissions
Civil Service Commissions
Education Administrators--Boards, Secondary Schools, Colleges, Universities
Fish & Game Commissions
Health & Sanitation Commissions
Information Centers
Insurance Administrations
Internal Revenue Administrations
Judicial/Court Systems
Law Enforcement & Public Safety Commissions
Licensing Commissions
Motor Vehicle Departments
Parole/Probation/Penal Authorities
Public Utilities Commissions
Treasury Departments

(2) County/Municipal:

Attorneys & Prosecutors
Clerks, Agents & Recorders (Births, Marriages, Divorces, Deaths, Property, etc.)
Consumer Affairs Agencies
Coroners & Medical Examiners
Courts
Election Boards
Financial Agencies
Fire Departments & Marshals
Housing Authorities
Inspection & Licensing Agencies--Health, Sanitation, Building, Professional, Occupational, etc.
Marriage License Bureaus
Motor Vehicle Departments
Police Departments & Sheriff's Offices
Public Libraries
Public School Administrations
Public Welfare Agencies
Public Works Departments
Purchasing/Procurement Agencies
Social Service Agencies
Tax Assessors

Trade, Industrial & Professional Commissions
Transportation Authorities
Truant Officers
Waterfront Commissions
Workman's Compensation Boards

6-3.4. PRIVATE AND COMMERCIAL RECORD SOURCES. The following is an incomplete list of private sources of recorded information. Due to the broad range covered, no attempt is made to describe what information might be available from each source; the list is intended to give a perspective and aid in selecting potential avenues of inquiry and exploration pertinent to an investigative problem:

American Red Cross
Automobile Associations:
American Association of Motor Vehicle Administrators
American Automobile Association
American Trucking Association
National Auto Theft Bureau
National Automobile Dealers Association
National Drivers Registration Service
Automobile Rental Firms
Banks & Financial Loan Companies
Civic, Charitable Religious, Fraternal & Vocational Organizations
Commercial Credit Organizations
Consumer Agencies & Better Business Bureaus
Credit Unions
Dunn & Bradstreet
Foreign Trade Organizations
Hospitals and Medical Service Organizations
Hotel Associations
Insurance Agencies & Investigative Firms--Life, Health, Casualty, Fire, Automobile, Marine, etc.
Private/Special Libraries & Information Centers
Public Utilities Companies--water, gas, electric
Real Estate Agencies
Security/Protection Agencies
Telephone & Telegraph Companies
Trade, Industrial & Professional Organization
Transportation Companies--Air, railroad, bus, taxi, water

6-3.5. TWO KEY COMMERCIAL DATABASES

a. Choice Point owned Autotrack XP (ATXP) is a commercial database that contains over 13 billion records. The database, which uses multiple inputs, is constantly updated to provide information on a real-time basis. The key inputs to ATXP are name, SSN and DOB. If SSN is not known, queries are possible based on name and DOB or

name only. Queries are also possible based on known name and address, a last name and a street name, name and ZIP code, and other data combinations. The strength of ATXP is the size of the database and the constant updating of information. ATXP is available directly to field units. Each office has a number of personnel with ATXP accounts to permit field personnel to access the information at any time.

b. Lexis-Nexis (L-N) is another commercial database used to assist investigations. L-N, which is only available through NCISHQ Criminal Intelligence Division, does not have the number of inputs as ATXP; however, L-N has an extensive law library and print media database, which is unavailable in ATXP. L-N queries are made in Boolean language, which gives the user greater flexibility when minimal known information is provided.

6-3.6. MISCELLANEOUS SOURCES OF REFERENCE. The following are samples of reference sources, which may be of direct or indirect investigative value:

City and Street Address Directories
Library Reference Books
Guide to American Directories
Directory of Special Libraries & Information Centers
World Aviation Directory
Biographic Reference Books
Book Review Digest
Readers Guide to Periodical Literature
International Index to Periodicals
New York Times Index
Public Affairs Information Service
Index to Legal Periodicals
Agricultural Index
Index Medicus
Business Periodical Index
Applied Science and Technology Index
The Standard Periodical Directory
Guide to Reference Works
Newspaper Files (Morgues)
Real Estate Directories
Telephone Directories

6-4. STATEMENTS

6-4.1. Oral statements of witnesses, including victims, or of an accused should be reduced to writing immediately after the interview or interrogation. While oral testimony may be valid in every respect, the difficulty arises in later when attempting to prove what was stated. Thus, it is important to preserve oral statements by reducing them to writing. It is a standard policy requirement in NCIS, whenever credible information is developed which may be used in an administrative or judicial hearing, to ask the individual at the conclusion of the interview if he/she will furnish a written statement, preferably under oath. This statement

should be requested only after the interview has been completed. It is important that no pressure be applied by the agent to obtain a written statement. The request for a written statement at the conclusion of an interview should be treated by the agent as a normal and casual follow-up to his contact with the person concerned. It is important that no issue be raised between the agent and the individual over the submission or non-submission of a written statement by the latter. Merely pointing out that a written statement precludes the possibility of misquotes, etc., is frequently successful. The employment of a high degree of tact by agents in soliciting a statement is essential. If an individual refuses to make a statement, this fact should be included in the Report of Investigation (ROI).

6-4.2. In connection with statements in criminal type cases or in any case where administrative or judicial action is likely to be taken against the person making the statement, the requirements of Article 31b, Uniform Code of Military Justice (UCMJ) must be met. This is essential in the case of any person suspected of an offense who is subject to the Code since failure to comply will render the statement inadmissible before a court-martial. Specific warning and guidance procedures and information are set forth in NCIS-3 Chapter 7.

a. Where the person being questioned is not subject to the UCMJ, Article 31 is not applicable.

b. Occasions will arise where there is some doubt whether to "warn" an individual under Article 31, UCMJ, or the Fifth Amendment to the U.S. Constitution.

EXAMPLE: A Naval Reservist whose orders stipulate that he/she is/was subject to the Uniform Code of Military Justice while in training. Even though he/she is a civilian and subject to the Fifth Amendment, he/she may also be subject to the Uniform Code of Military Justice. Prior to interview, agents should determine the subject's status in order to accomplish the appropriate "warning." Dual "warnings" under both Article 31, UCMJ and the Fifth Amendment are not required and should not be given.

6-4.3. There are two generally acceptable formats for statements. The designated format is dependent upon the circumstances of the case, such as, the disposition, age, attitude of the person being interrogated, availability of stenographic personnel, and ability of the person making the statement to write legibly and lucidly. Generally, handwritten statements, especially by victims and witnesses left to write their statements unattended, are incomplete in the detail needed for the investigation. As a matter of preferred practice, statements should be prepared by the special agent and typed whenever possible and appropriate; however, a handwritten statement is fine if the interviewing special agent works with the interviewee to ensure all the details are included. The two formats for statements are Narrative Form and Interrogatory (Question and Answer) Form.

a. Narrative Form, Appendix 1. When a statement is made in narrative form, it should be, insofar as possible, in the maker's own words. If the subject requests the agent or another person to write or type the statement for him/her, the text of the statement should show that he/she requested this accommodation. Microsoft investigative form templates

provide the NCIS Representative a standardized and legally sufficient format to record statements.

b. Interrogatory (Question and Answer) Form, Appendix 2. The question and answer type statement provides an accurate record of the subject's responses in his/her own words to pertinent questions. When the statement is in question and answer format, the same essential elements are required as for the Narrative Form statement.

6-4.4. The following procedures are recommended in taking statements from persons accused or suspected of offenses:

a. Do not undertake any interview until you have enough information from other sources to reasonably assure a successful outcome,

b. Get the subject talking and pace the interview according to his/her displayed characteristics,

NOTE: One proven approach is to ask questions regarding family background, past duty stations, etc., which the subject will probably answer readily.

c. Be persistent, but patient, and

d. Get the statement signed as soon as possible.

6-4.5. Mistakes commonly found in recording statements are:

a. Insufficient detail,

b. Delaying preparation of the statement to a more convenient time,

c. Using language unlike that habitually used by the subject,

d. Failing to document the statement with initials and attestation clause.

e. Incomplete identification of other individuals/suspects mentioned by the maker in his statement,

f. Failing to elicit all available evidence held by the maker against such person. Each element of the applicable offense should be covered,

g. Failing to include factual data (dates, times, places) that will support a specification of an offense,

h. Failing to include the date and local time when the statement was taken, and

i. Failing to include signature of witnesses or jurat.

6-4.6. Each NCIS Representative present should witness the signature of the maker. In order to preclude any later claim by the person making the statement that it was signed under duress or undue influence, officers or enlisted personnel senior to the maker should not be present or witness a statement. When interrogating a woman, it is desirable to have another woman present in lieu of another agent or male witness. Specific instructions regarding the interrogation of female service personnel are set forth elsewhere in NCIS-3 Chapter 14.

6-4.7. OATHS IN CONNECTION WITH STATEMENTS

a. Under instructions promulgated by the Secretary of the Navy (currently SECNAV Instruction 5430.107) duly accredited Representatives of the Naval Criminal Investigative Service have authority to administer oaths in the performance of their official investigative duties. Title 5, U.S. Code, section 303 (Oaths to Witnesses) states "...an employee of the Department of Defense lawfully assigned to investigative duties may administer oaths to witnesses in connection with an official investigation."

b. At a Pre-Trial Investigation (Article 32, UCMJ) a written statement of witness, not present, may be considered only if they have been obtained under oath or affirmation. Whenever practicable in criminal investigations, it is necessary that statements obtained from witnesses be sworn statements. Because there are increasing requirements for sworn statements in other than criminal cases, it shall be the general rule that written statements obtained by NCIS agents shall be taken under oath, whenever practicable, except where circumstances render such procedure unnecessary. In most cases, the NCIS Representative will administer the oath after the statement has been obtained and reduced to writing. Should the author of a statement decline to be sworn, his un-sworn statement shall be accepted. The report shall indicate the fact that the statement is un-sworn and give the reason.

c. Under certain circumstances it may be desirable to place a witness under oath at the outset of the interview, particularly where the witness, whether cooperative or hostile, is expected to furnish significant derogatory information. The foregoing must not be construed as requiring that an individual be sworn. Indeed, an agent has no authority to order any individual to take an oath; this must be an entirely voluntary procedure. Circumstances under which a witness might be sworn at the beginning of an interview should be limited to instances where it is clearly indicated that the individual intends to impart information and is willing to be sworn, while knowing that he/she has an opposite choice.

d. There is no legal requirement that the written statement of an accused must have been taken under oath for it to be admissible into evidence in a trial by court-martial. The governing factors for admissibility are that the statement be truly voluntary and a proper warning preceded it. It is desirable that the statements of suspects be taken under oath whenever feasible; the agent shall always afford an opportunity to a suspect making a statement to make it under oath.

6-4.8. PROCEDURE FOR ADMINISTRATION OF OATHS

a. Whether an oath is administered at the outset of an interview, as stated in Section 6-4.7 or at the conclusion of a written statement, it should be completed with a formality befitting the occasion. At the time the oath is administered, the affiant and the person administering the oath must be in each others' presence. As stated in the Manual for Courts-Martial, United States, 2005 there is no particular procedure that must be used in administering the oath. Any procedure that appeals to the conscience of the person to whom the oath is administered and which binds him/her to speak the truth is sufficient. Customary procedures include requiring the person taking the oath to place a hand upon a Bible while the oath is administered or raising the right hand by both the individual administering the oath and the person taking the oath at the time of reciting thereof and the response thereto. In most cases, the second procedure above will be the most practicable for the NCIS Representative and, in general, shall be employed unless there is good reason to the contrary. Persons who recognize other forms or rites as obligatory, and believers in other than the Christian religion may be sworn in their own manner or according to the ceremonies of the religion they profess and which they declare to be binding.

b. The Manual for Courts-Martial (MCM), United States, 2005 does not contain an explicit form of oath for use in connection with the statements of witnesses taken outside the judicial procedure as contemplated herein; however, there is legal authority which states that in this situation the form of oath prescribed for witnesses in an Article 32 investigation may and should be utilized. This form is as follows: "You swear (or affirm) that the (statement given by you is) (evidence you are about to give shall be) the truth, the whole truth, and nothing but the truth. So help you God." An affirmative response validates the oath.

NOTE: In the case of affirmation, the words "So help you God" are omitted.

c. Where a written, sworn statement, also called an affidavit, is obtained, it is to be authenticated by the NCIS Representative who administers the oath after the affiant has signed it and has been duly sworn. The following form of jurat shall be used:

Sworn to and subscribed before me this _____day of
_____ in the year_____
at_____

_____
Representative, Naval Criminal Investigative Service
AUTH: DERIVED FROM ARTICLE 136, UCMJ
(10 U.S.C. 936) AND 5 U.S.C. 303

WITNESS:

_____

d. The authority conferred on NCIS Representatives to administer oaths is intended to be applicable only to those persons who are regularly assigned to investigative duties, including supervisory personnel. It shall not be used as a basis for requesting the issuance of credentials to other persons not engaged in investigative duties in order to provide them with authority to administer oaths.

6-4.9. DOCUMENTING THE RESULTS OF AN INTERVIEW OR INTERROGATION. When a victim, witness or suspect provides information, but a statement is not reduced to written form, the results will be reported via Investigative Action (IA) format (see NCIS-1, Chapter 25). This IA should contain all the details provided by the interviewee, including what rights, if any, were advised and why a written statement was not executed. In the case of suspects who waived their rights in writing, the acknowledgement and waiver of rights form should be appended to the IA.

6-4.10. POLICY FOR USING THE COMPUTER TO TAKE STATEMENTS

a. To avoid having the agent's hard drive seized and forensically examined, apply the following policy when using a computer or any other digital device to record a witness/subject's written statement:

(1) Do not invite or permit the subject/witness to review the statement by looking at the computer screen while it is being prepared or edited. As a standard practice turn the computer screen away from the subject/witness as the statement is being prepared.

(2) After the agent is satisfied that the prepared statement accurately reflects the facts as the witness/subject has presented them, PRINT OUT a HARD COPY of the statement and it to the witness/subject for review. If the witness/subject wishes to make any changes, provide him/her with a pen to make any changes on the hard copy as it is being reviewed. The witness/subject should initial the beginning and end of each paragraph, as well as, any pen and ink changes.

(3) Only if the pen and ink changes make the statement illegible should the statement be electronically and provide the witness/subject with a second version for review, again following the same procedure in paragraphs 4.a. and 4.b. above. The agent should note on the printed statement that the pen and ink changes made by the witness/subject are incorporated in the second version of the statement for the purposes of clarity and legibility and have the accused initial that notation.

(4) Save the printed hard copy of the statement with the pen and ink changes made by the witness/subject in the case notes. The agent should also save ALL other contemporaneous documentation of the witness/subject's statement (i.e. interview notes and any other printed versions of the statement that the witness/subject has reviewed) with the case notes.

b. By following the above process, the agent will avoid the seizure and forensic examination of his/her computer hard drive as a result of the very common defense request for prior statements by a witness or accused. This process can also prevent unnecessary delay in bringing the accused to justice by saving the convening authority and trial counsel the significant time and resources necessary to answer a legal issue that could easily be avoided. By accurately and properly recording the facts a witness/subject provides during an interview, the agent can prevent a situation where it is his/her word against the accused's during trial without any evidence to support the agent's testimony.

6-5. INVESTIGATIVE NOTES

6-5.1. Notes are the tools used in building a case. They should supply information, which together with the statements and the documentary and physical evidence obtained during an investigation, to facilitate preparation of a complete report.

6-5.2. The method of taking notes will be left to the discretion of the agent as long as the notes identify persons interviewed, their residence and business address, dates and places of interview, and reflect all pertinent material information developed. Notes should always be comprehensive, accurate, and neat.

6-5.3. More detailed notes concerning the substance of pertinent information developed are required when no signed statements are obtained. When signed statements are obtained, the notes need not repeat the substance of the statement but should supplement it by with any pertinent information not included in the statement.

6-5.4. Recording only one interview per sheet of paper will permit flexibility of handling when interview results are being arranged in logical order for report preparation. This practice will also assist in confining use of notes at a trial to just those that relate to a particular subject matter.

6-5.5. When interviewing responsive witnesses, it may be expedient to make notes during the interview. Such persons are usually anxious to impart information and will not object to being recorded and will consider note taking as an acknowledgement of the importance of what they have to say.

6-5.6. When interviewing hostile, indifferent, or doubtful witnesses, the agent generally should not produce his/her notebook until he/she is satisfied that the person has first orally related all pertinent information. The agent can then record the pertinent information in either or both statement or note form; the person interviewed can be assured that such procedure serves as a protection for him/her in providing an accurate record of the orally furnished information.

6-5.7. Lengthy interviews may require the taking of copious notes long before the person interviewed has first orally covered all pertinent information. In such cases a notebook or pad might be produced for the purpose of recording a number, formula, amount, or similar information that the agent would not normally be expected to remember.

6-5.8. If notes are not made during the interview they should be made immediately after the interview while the conversation is still fresh in the agent's mind.

6-5.9. Identification of notes by dating, initialing, and placing the case file number on each page will prevent intermingling of notes relating to different cases and, when necessary, will permit use at trial.

6-5.10. Inspection of the notes of agents assisting in an investigation should be made by the "Case or Control Agent" in charge of the investigation to assure maintenance of proper notes. One method to preserve notes is to place them in an envelope appropriately labeled and file them with exhibits obtained during an investigation or at least until such time as the case is disposed of or is certain that no further use of them will be necessary. Full and complete notes are essential for effective investigation and good investigative reports. Although note taking should never be allowed to hinder progress of an interview, the agent should make accurate notes, abbreviating if necessary, of material pertinent to the investigation. When a person refuses to talk because notes are taken, the agent should complete the interview as previously mentioned and later record all pertinent information while it is fresh in his mind, at the first convenient opportunity following the interview.

6-5.11. JENCKS ACT MATERIAL. The Jencks Act provides, in part, that after a government witness has testified on direct examination, the court shall, on motion of the accused, order the production of any statement of the witness, in the possession of the United States, which relates to the subject matter to which the witness testified. (See 18 USC 3500.) Failure of the government to comply with the order to produce the statement will result in the testimony of the government witness being stricken from the record. The term statement is used in its broadest sense. When a written recorded observation, no matter how informal, is transferred to a government agent for the purpose of imparting information and is orally verified by its author as to its truth and accuracy, the writing becomes a statement as contemplated by the Jencks Act and is destroyed by the government at its peril. All statements, notes, drawings, outlines, and other transcribed or recorded information (i.e. tapes of a dictated statement) which come into the possession of a special agent during the course of an investigation and might be conceived of as being adopted or verified by a potential witness for the government, must be retained with the case notes. Should the suspect be convicted at trial, the case notes should be preserved until the case has been processed through the appeal system. Questions regarding specific matters concerning a particular trial should be addressed to the prosecuting attorney, trial counsel, or NCISHQ (00L) as appropriate.

6-6. REFERRED INVESTIGATIONS

6-6.1. Inherent in the NCIS investigative and liaison role in criminal and counterintelligence matters is a responsibility to ensure that those investigations of interest to the Department of the Navy or higher authority which are referred by NCIS to other agencies are adequately resolved and promptly reported to the command concerned. (The term "referral", in this section, also includes all cases in which another agency is apprised or consulted, and

assumes primary investigative jurisdiction. The mandates of this section are not limited to those cases referred under the 1984 DOD/DOJ Memorandum of Understanding (DOD Directive 5525.7). NCIS can appropriately discharge this responsibility by strict adherence to a policy, which provides for:

a. Retention of control and active involvement until the investigation is actually assumed by the other agency;

b. Continuing close liaison, with written tracer follow-up as necessary, until investigative action is completed;

c. Uniform procedures for referring, documenting and reporting such investigations;

d. Keeping their investigation in a pending status until all investigations are completed by the agencies involved when matters are a Department of the Navy interest, e.g., where a service member is a suspect or where the Navy is victimized or its operations are affected.

6-6.2. NCIS components will maintain an active role, usually by concurrent investigation or through continuing liaison, in all referred investigations until action is completed and reported to the interested command.

a. To preclude loss of continuity and delay in completion of referred investigations, NCIS shall continue the investigation, solely or concurrently, until an affirmative determination has been made by the other agency that investigative interest does exist and positive steps are taken by that agency to assume investigative jurisdiction. Special attention to continuity should be given those referred investigations in which the U.S. Attorney characteristically finds no prospective interest.

b. Notwithstanding such arrangements, there will be cases in which an investigation, initially assumed by another agency, is terminated by that agency prior to resolution. In such cases, NCIS shall promptly report the actions taken by the other agency to the command concerned for a determination as to whether or not further investigation is necessary to enable command to take appropriate disciplinary, administrative or other action. Should further investigation be deemed necessary, it shall be conducted by NCIS or referred by NCIS to other authorities as appropriate.

c. The NCIS component making the referral, usually the NCISRA, shall affect a continuing and aggressive follow-up in each referred investigation. Initial personal liaison shall be succeeded by written tracer action in each case in which the other agency fails to respond or report within a reasonable time (no more than 90 days). A separate chronological "tickler" file will be maintained by the referring component and will be discarded upon receipt of the final report from the other agency.

d. In each case that requires prompt notification (referral or advisory) to another agency, the mode of initial communication shall be appropriate to the urgency of the

situation. However, it is mandatory that all referrals, assumptions and declinations of jurisdiction be documented and made a matter of record in NCIS Central Files.

6-6.3. All referrals of investigations properly of interest to the Department of the Navy or higher authority (i.e., results thereof are to be reported to the command concerned) shall be documented by Report of Investigation (ROI). Investigative effort will be considered expended in each such referral even though the initial investigation comprises only the interview of a complainant, a "walk-in" source or a command representative. Results of preliminary inquiries already completed by command investigators, if properly accomplished and adequately reported, may be documented by inclusion of such report as an exhibit to the NCIS ROI.

6-6.4. The ROI documenting the initial investigation and referral shall serve as the written notification to the other agency.

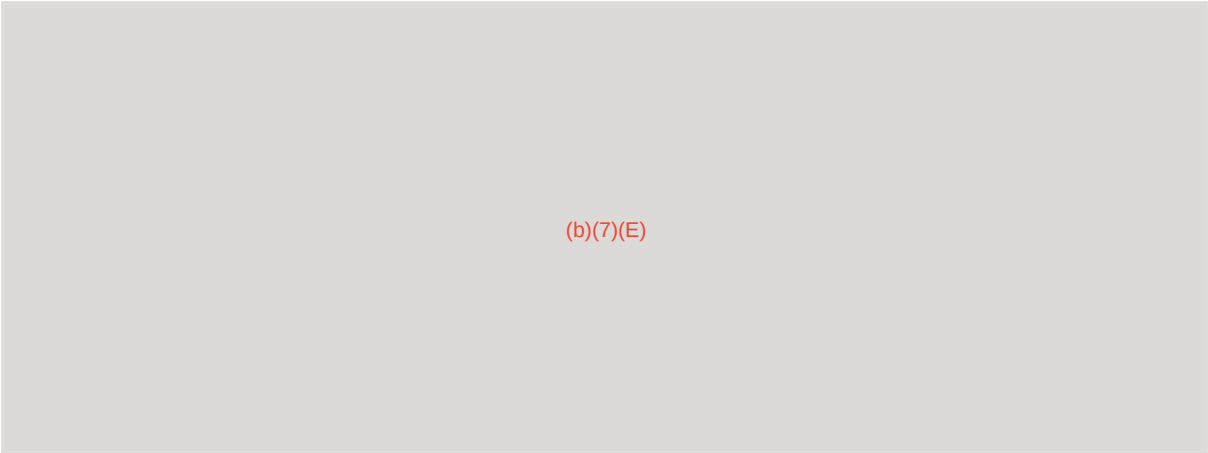
6-6.5. Reports of investigation and/or advice as to action taken by the other agency shall be forwarded to NCISHQ by ROI for inclusion in NCIS Central Files. A copy of the other agency's report or advice as to action taken shall be provided also to the interested command, as necessary, in accordance with existing policy governing transmittals.

6-7. MAIL COVERS

6-7.1. U.S. Postal Service Publication 55 outlines the procedures for initiating, processing, placing, and using mail covers. The sole authority for mail covers is provided in title 39, Code of Federal Regulations, section 233.3. All concerned personnel should be thoroughly familiar with those provisions with respect to the use of mail covers as an investigative technique, the prescribed conditions that must be met, and the procedures for making such a request.

(b)(7)(E)

Page 90 redacted for the following reason:
- - - - - - - - - - - - - - - - - - - -
(b)(7)(E)



6-8. HOTLINE COMPLAINT INVESTIGATIONS

6-8.1. The Naval Inspector General (NAVINSGEN) and the Inspector General of the Marine Corps (IGMC) initiate requests directly to NCISHQ for investigation based on Department of Defense (DOD) and General Accounting Office (GAO) Hotline complaints. Additionally, NAVINGSGEN manages and controls the Navy Hotline Program and will initiate requests directly to NCISHQ based on those complaints. NCISHQ will prepare a ROI (INFO) and forward the information to the appropriate NCISFO for response by ROI (INFO) or by submitting a ROI (OPEN). These investigations will be Priority (II).

6-8.2. A hotline complainant who has been identified, but wishes to remain anonymous, will be treated as an Identity Protected Witness. A written copy of each DOD, GAO or Navy hotline complaint is usually provided to NCISHQ and will, absent unusual circumstances, be provided to the lead NCISFO(s). There are no restrictions on allowing the cognizant command to review the complaint or to make it an exhibit to resulting ROIs if the identity of the cooperating witnesses is protected.

6-8.3. To allow for more efficient control and retrieval of hotline investigations, project indicators "NH", "MH", and "DH" are used in the CCN of all investigations originating from a DOD, GAO or Navy Hotline complaint. The "NH", "MH", and "DH", project indicators should not be used in investigations resulting from complaints received through command-sponsored hotlines. NCIS-1, Chapter 25 provides additional guidance.

6-9. GRAND JURY MATTERS

6-9.1. BACKGROUND. The grand jury process exists as primary security to the innocent against hasty, malicious and oppressive prosecution. Under the Fifth Amendment to the Constitution of the United States, "no person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment by a Grand Jury..." Rule 7, Federal Rules of Criminal Procedure (FRCP), requires that an offense punishable by imprisonment for more than one year must be prosecuted by indictment unless indictment is waived. The Fourteenth Amendment to the U.S. Constitution does not require States to initiate criminal prosecutions by grand jury indictment.

Pages 92 through 99 redacted for the following reasons:
- -
(b)(7)(E)

(b)(7)(E)

6-11.2. DODIG Subpoena preparation and procedures are detailed in NCIS-6, Chapter 14. Forms used in the subpoena process can be found on-line under the NCIS intranet homepage http://infoweb.ncis.navy.mil/23a/subpoena_templates.htm
Clicking on Departments under Info-web homepage and choosing Economic Crimes can reach this site.

6-12. RIGHT TO FINANCIAL PRIVACY ACT

6-12.1. The Right to Financial Privacy Act, 12 U.S.C. Section 3421 (B) of 1978. (See 12 USC 3401) governs Government access to financial records and directs this information be submitted to Congress annually. The purpose of the Act is to protect customers of financial institutions from unwarranted government intrusion while at the same time permit legitimate law enforcement activity. Basically, the Act provides that records from a financial institution may be obtained by one of five authorized means: (a) valid written customer authorization; (b) administrative summons or subpoena; (c) valid search warrant; (d) judicial subpoena; or (e) formal written requests. A financial institution is generally prohibited from releasing a customer's financial records until the federal agency seeking the records certifies in writing to the financial institution that it has fully complied with the Act.

6-12.2. It is important to note that only a narrow class of records is covered by the Act (i.e., "financial records" pertaining to a "customer" obtained from a "financial institution"). Institutions not covered by the Act include: bonding companies, credit bureaus, the U.S. Postal Service, and Western Union. Financial records not covered by the Act include: forged or counterfeit financial instruments; records relating to an account established under a fictitious name; and contents of a safe deposit box sought pursuant to a search warrant. Access to basic identifying account information, limited to name, address, account number, and type of account, is permitted by means outside of the above five access mechanisms. (enclosures (2) and (9) to DOD Directive 5400.12 which is an attachment to SECNAVINST 5500.33.)

6-12.3. DOD Directive 5400.12 of 6 February 1980 and SECNAVINST 5500.33 of 23 June 1980 implement the Right to Financial Privacy Act for the Department of Defense and the Department of the Navy and apply to all NCIS special agents seeking access to financial records maintained by financial institutions.

6-12.4. NCISFO ANNUAL REPORTS REQUIREMENT. Pursuant to the requirements of SECNAVINST 5520.33 and the law underlying the Instruction, each NCISFO is tasked with compiling an annual report setting forth the details of Government use of this technique. The report shall be prepared on DD Form 2563, JUN 92 entitled “DEPARTMENT OF DEFENSE RIGHT TO FINANCIAL PRIVACY ACT OF 1978”, and submitted to the Special Assistant for Legislative & Judicial Affairs (NCISHQ –000L) by 15 January each year.

6-12.5. A detailed discussion of the Right to Financial Privacy Act will be found in NCIS-6, Chapter 4.

6-13. FAIR CREDIT REPORTING ACT

6-13.1. The Fair Credit Reporting Act requires that consumer reporting agencies adopt reasonable procedures to protect the confidentiality, accuracy, and proper use of credit, personnel, insurance, and other information collected for use in the commerce of the United States (see 15 USC 1681). The Act imposes certain restrictions on both credit and consumer reporting agencies and users. The Act defines consumer reporting agency as any person or organization which, for monetary fees, dues, or on a cooperative non-profit basis; regularly engages in the practice of assembling or evaluating consumer credit or other information for the purpose of furnishing that information to third parties. The Act provides for both civil and criminal penalties for violations by the consumer reporting agency and the user. Those sections of the Fair Credit Reporting Act that affects investigations conducted by special agents of this Service can be found at 15 USC 1681b. Permissible purposes of reports: A consumer reporting agency may furnish a consumer report under the following circumstances and no other:

a. In response to the order of a court having jurisdiction to issue such an order,

b. In accordance with the written instructions of the consumer to whom it relates, or

c. To a person, which it has reason to believe the following intentions:

(1) To use the information in connection with a credit transaction involving the consumer on whom the information is to be furnished and the extension of credit to, review or collection of an account of, the consumer;

(2) To use the information for employment purposes,

(3) To use the information in connection with the underwriting of insurance involving the consumer,

(4) To use the information in connection with a determination of the consumer's eligibility for a license or other benefit granted by a governmental instrumentality required by law to consider an applicant's financial responsibility or status, or

(5) Has a legitimate business need for the information in connection with a business transaction involving the consumer.

6-13.2. DISCLOSURE TO GOVERNMENTAL AGENCIES. Notwithstanding the provisions of 15 USC 1681b, a consumer reporting agency may furnish identifying information respecting any consumer, limited to name, address, former addresses, places of

employment, or former places of employment, to a governmental agency. (See 18 U.S. Code 1681f.)

6-13.3. With the exception of present and former addresses and employment authorized in section 1681f, consumer reporting agency information will not be solicited by NCIS personnel or reported in NCIS documentation unless the requirements of section 1681b have been met, i.e. court order or customer consent obtained. Any use of consumer reporting agency information which is authorized by that section, i.e. information collected during a pre-employment investigation of an agent applicant or any investigation of an NCIS employee, is reportable in NCIS documentation.

6-14. EYEWITNESS IDENTIFICATION

6-14.1. GENERAL. The identification of criminal offenders by eyewitnesses is one of the most important techniques available to agents in apprehending and convicting Federal law violators. The eyewitness' in-court testimony will be of little value if it is suppressed because of improper pretrial identification procedures or is subject to impeachment because of questionable practices used by the special agent when the pretrial identification was obtained. The following guidelines have two important purposes: to assure the admissibility and credibility of eyewitness identification testimony and to make certain that all identifications are the product of the honest, independent recollection of the witness. These rules reflect and incorporate constitutional requirements as interpreted by the Federal courts and the Military Rules of Evidence (MRE). In addition, policy considerations have been included which are believed helpful in achieving the purposes stated above.

6-14.2. LINEUPS.

a. When Conducted. A lineup should be held only when clearly necessary. Such a case is one in which identification by a witness is a critical factor and the witness is so unfamiliar with the accused that identification is uncertain. Other significant factors, which may be considered by the agent in making a determination of whether to conduct a lineup, are:

(1) Other Evidence. If the Government possesses a significant amount of other evidence, such as an admission of a codefendant, a confession, or physical evidence, eyewitness identification may be unnecessary and consideration should be given to foregoing a lineup. This is especially true when the eyewitness' recollection is weak.

(2) If the witness relates the inability to specifically identify the suspect even if see again in a lineup.

(3) Unusual Appearance of Suspect. If the suspect's appearance is uncommon or unusual and difficulty is experienced locating suitable elimination participants, consideration should be given to not holding a lineup.

(4) Prior Knowledge. If the witness is acquainted with the suspect and recognized him/her during the offense, a lineup may be unnecessary.

(5) Inconvenience. If the suspect is in custody a great distance from the witness, a lineup may not be feasible. Consideration should be given to using photographic identification procedures.

(6) Uncooperative Suspect. It may be unwise to hold a lineup if the defendant threatens disruptive tactics.

(7) Consultation with Trial Counsel or U.S. Attorney. If there is any uncertainty about the necessity or wisdom of conducting a lineup, the agent should seek the advice of the U.S. Attorney (USA) or Trial Counsel (TC).

b. Defense Objections to Proposed Lineups. If defense counsel raises objections or in any other manner obstructs the proposed lineup, defense counsel should be advised to discuss the matter with the USA or TC.

c. Right to Counsel.

(1) Civilian. The legal right to the presence of a lawyer at a lineup exists only if the lineup takes place after arrest or the initiation of formal prosecution and the lineup is connected with the offense for which the suspect has been arrested or charged. This is true whether the arrest is made with or without a warrant and whether the filing of a complaint or information, or the return of an indictment initiates prosecution.

(2) Military. Military Rule of Evidence 321 provides: "An accused or suspect is entitled to counsel if, after preferral of charges or imposition of pretrial restraint ... for the offense under investigation, the accused is subjected by persons subject to the code (UCMJ) or their agents to a lineup for the purpose of identification. When a person entitled to counsel under this rule requests counsel, a judge advocate... shall be provided by the United States at no expense to the accused or suspect and without regard to financial standing or lack thereof; before the lineup may proceed. The accused or suspect may waive the rights provided in this rule if the waiver is freely, knowingly, and intelligently made."

d. Lineups Prior to Arrest or Initiation of Prosecution.

(1) Civilian. If a civilian suspect voluntarily appears in a lineup before the arrest or initiation of prosecution or is compelled to appear per a court order or grand jury subpoena, he/she shall be informed that counsel may be retained for the lineup if so desired; however, he/she has no legal right to counsel, and one will not be appointed to represent him/her.

(a) Lineup Acknowledgement and Waiver of Rights. If the suspect fails to retain counsel, it is not necessary to obtain a waiver or execute NCIS Form 5580/16(1/2001)

Lineup Acknowledgement and Waiver of Rights (Civilian), formerly NISFORM 036. The lineup may be held without the presence of a defense attorney.

(2) Military. Military suspects need not be advised that they may have an attorney at the lineup if charges have not been preferred or pretrial restraint has not been imposed for the offense under investigation.

e. Lineups After Arrest or Initiation of Prosecution, Civilian and Military.

(1) Unrelated Offenses. Even after the initiation of criminal charges, a suspect does not have the right to counsel at a lineup relating to other criminal offenses that have not been formally charged. For example, if a suspect is arrested/apprehended and charged with assault and is subsequently developed as an auto theft suspect, he/she would have no legal right to be represented by counsel at a lineup held for witnesses of the auto theft.

(a) If such a lineup is contemplated, the civilian suspect should be informed well in advance of the lineup that he/she has no legal right to an attorney at the lineup and one will not be appointed for representation. If retained or appointed counsel, or desires to hire an attorney already represent the civilian suspect, he/she should be permitted to do so and have the attorney at the lineup to represent him/her. If the civilian suspect fails or declines to retain counsel, the lineup may proceed without the presence of a lawyer for the suspect. In that event, it is unnecessary to obtain a waiver or execute NCIS Form 5580/16(1/2001) Lineup Acknowledgement and Waiver of Rights (Civilian).

(b) The military suspect need not be told that he/she may obtain the services of a civilian or military attorney under these conditions. Also see section 0705.4.g, NCIS 093, if an interrogation is planned after the lineup.

(2) Same Offense. Civilian and military suspects have the right to a lawyer for any lineup in connection with the offense for which they have been arrested (civilian), or charged (military) or placed in pretrial restraint (military). If they cannot afford one, they have the right to have one appointed. No lineup shall be held under this section if the suspect is not represented by counsel or refuses to execute a waiver of counsel.

f. Waiver of Counsel.

(1) Lineups After Arrest/Apprehension or Referral of Charges. If the accused or defendant has no counsel at the time of the lineup or counsel has not appeared, the defendant should be asked if he/she is willing to appear in the lineup without the benefit of counsel. If willing, he/she should be requested to waive counsel by signing NCIS Form 5580/16(1/2001) Lineup Acknowledgement and Waiver of Rights (Civilian) or NCIS Form 5580/17(1/2001) which is used for Military.

(2) All investigative forms to include the above are in Microsoft Word templates.

(3) Refusal to Sign Form. If the suspect is willing to appear without counsel, but will not sign the form, his/her words should be written in the blank space below the signature line on the form. Two witnesses should then sign the form and the lineup held.

(4) Voluntariness of Waiver. To be valid, the waiver must be voluntary. Agents should not do or say anything that would make the waiver anything other than the product of the suspect's free choice.

g. Substitute Counsel. If the suspect is entitled to a lawyer but is not represented by counsel and refuses to waive counsel, the USA or TC, as appropriate, should be asked to request the court or command to appoint counsel for lineup purposes. The lineup should not be conducted if the suspect is not represented by counsel and refuses to execute the waiver.

h. Role of Defense Counsel. The proper function of a defense attorney at a lineup is merely that of an observer. His/her presence is required to assure intelligent cross-examination of the lineup witnesses later at trial, and to detect anything that might affect the admissibility of testimony about the lineup.

(1) Lawyer's Suggestions. The defense lawyer should be permitted to make suggestions concerning the procedure of the proposed lineup. The agent should attempt to incorporate any reasonable suggestion, which promotes the fairness of the lineup. All suggestions, whether adopted or not, should be noted by the agent supervising the lineup and included in the Results of Lineup (ROL).

(2) Participation During Lineup. The attorney should be instructed not to converse with the lineup participants or witnesses during the lineup. Any attempts to disrupt the lineup should be noted by the agent in the ROI. If the attorney for the defendant obstructs the identification, he/she may be excluded from the lineup room. In the event a defense attorney is excluded, the USA or TC should be contacted before resuming the lineup.

(3) Presence at Moment of Identification. The witness should make the identification attempt while viewing the lineup formation. Defense counsel should be present, but should not be allowed to communicate with the witness at this time.

(4) Presence at Post lineup Interview of Witness. The right to counsel does not extend to interviews with lineup witnesses after the conclusion of the lineup. The suspect's lawyer should be excluded from the post lineup interviews of lineup witnesses.

(5) Contact with Government Witnesses After Completion of Lineup. The lineup witness may be told that he/she may speak with the defense attorney if he/she wishes, but is under no legal obligation to do so. The witness' name and address should not be revealed to the defense lawyer without the consent of the witness, unless the agent has been advised by the USA or TC to do so.

i. Suggested Lineup Procedure. Whether or not the suspect is in custody, the choice of the location for the lineup should be based upon considerations of maximum privacy and control of the lineup room. The lineup should be held in a well-lighted room with controlled entrances to insure that the identifying witness does not view the suspect prematurely.

(1) Number of Participants. The persons who will have roles in the executions of the lineup are: the controlling agents, the suspects, the identifying witness, and the persons who will appear in the lineup with the suspect (lineup selectees). Agent(s), who decide to hold the lineup, should initiate and control the lineup to the exclusion of other command or custodial personnel. When selecting the persons who will appear in the lineup with the subject, care should be given to choosing persons who bear a reasonable similarity to the suspect. At least six persons, including the suspect, should be included. All participants should be of the same race and sex and of similar appearance. These persons may be selected from ship's company, security personnel, personnel assigned to naval shore units, other personnel as available, or combinations thereof. Persons known to the witnesses should not be used as elimination participants in the lineup.

(2) Clothing. The lineup selectees and the suspect shall wear articles of clothing which are the same or similar in form and color. No insignia or indication of rank or rate shall be displayed unless all are wearing the same rank/rating. The lineup suspect may be compelled to wear distinctive clothing. All other participants must then wear similar attire.

(3) Voice Identification. The suspect may be compelled to speak for voice identification if all participants are required to state the same words or phrases. Lineup participants should be required to speak in the order of their lineup number. None of the lineup participants, including the suspect, should be required to identify himself/herself individually when being viewed by the witnesses.

(4) Lineup Positions. The lineup shall normally consist of five lineup participants and the suspect. The numbers 1 through 6 shall be assigned to these persons in any reasonable manner. After being brought into the lineup room, the participants and the suspect shall be formed in a straight line about a foot apart. The participants shall be positioned in the lineup in the order of their assigned numbers. The positioning shall be arranged so that the person assigned to position number one will stand to the extreme left of the lineup as it is viewed by the identifying witness.

(5) Photograph of Lineup. Front and profile (one side) photographs of the lineup participants should be taken and copies should be appended to the appropriate Reports of Investigation.

(6) Viewing Movements. After the identifying witness takes a position where the lineup can be viewed, the witness will be afforded the opportunity to have four views of the persons in the lineup: front, left side, rear and right side. To accomplish this, the persons in the lineup will be required to perform viewing movements. The viewing movements shall be performed at the same time by all persons, in response to the direction of the agent. The suspect can be compelled to make certain gestures or assume particular poses. All other

lineup participants will be required to do likewise in numerical order to execute the gestures or poses.

(7) Conduct of Agents. Agents participating in or observing a lineup should not do or say anything to call the witness' attention to the suspect. Agents should not comment on the validity of an identification made by a lineup witness.

(8) The Execution of the Lineup. The agents participating in the lineup should plan their respective responsibilities. Agent(s) controlling the members of the lineup shall bring the members into the lineup room and establish the lineup formation. He/she shall then stand away from the lineup and advises the other agent that the lineup is ready. The identifying witness shall then be brought into the lineup room or to the viewing window. The witness should face the lineup at a safe distance, accompanied by an agent who should take a position enabling him/her to provide for the witness's personal safety. At this point, the agent controlling the members of the lineup shall direct the members to execute the prescribed viewing movements, pausing between commands. After completion of the movements, and any required voice identification, gesturing, etc., the members will be facing the witness. The agent controlling the identifying witness should then ask the question: "Do you recognize anyone?" If the response is negative or indeterminate, the lineup shall be terminated unless the witness asks for additional movements, voice identification, gestures, etc. If the witness' reply is in the affirmative, the witness should be permitted to identify the person in his/her own words, e.g., "The second man from the right (or the left, or #2) attacked me." The agent should then ask (but not by name) the designated person to take a step forward. After the person has stepped forward, the agent controlling the witness should ask the witness the question: "Do you identify that (the person who stepped forward) individual?" After the witness answers the question, the procedure shall be terminated. The witness should be escorted from the room or the viewing window. In the event of a positive identification, the witness should be asked to execute a signed, sworn statement setting forth the reasons for the identification.

(9) Multiple Witnesses. Multiple witnesses should view the lineup separately. Care should be taken to segregate the witnesses during the lineup so that they are unaware of the reactions of the other witnesses.

j. Lineups Conducted by Local Authorities. It is recognized that in some instances local police facilities and personnel might have to be used to conduct a lineup. In that event, efforts should be taken to assure that the procedures used by the local authorities substantially conform to the procedures outlined above.

k. Refusal to Participate. An in-custody suspect has no right to refuse to participate in a lineup. If a suspect refuses to participate or refuses to perform required acts in the lineup (utter certain words, perform certain acts), he/she should be informed that he/she has no right to refuse. The defendant may be informed that evidence of his/her refusal might be used against at trial. If the suspect continues to refuse, consideration should be given to obtaining a military or a court order to compel participation, or employing photographic identification procedures.

l. Detention of Suspects for Lineups. When probable cause for arrest is not present, or when an arrest is not desirable, these possibilities are available to compel the suspect to appear in a lineup:

(1) Court Order. Upon approval of the U.S. Attorney, an affidavit may be filed with the U.S. Magistrate or U.S. District judge seeking an order compelling the suspect to appear at a designated place and time for a lineup. The affidavit should contain facts establishing grounds to believe that a federal offense has been committed, there is reason to suspect that the person named or described in the affidavit committed the offense, and the results of the lineup will be of material aid in determining whether the person named in the affidavit committed the offense.

(2) Grand Jury Subpoena. The U.S. Attorney may be requested to ask the Federal grand jury for a subpoena directing the suspect to appear in a lineup at a designated time and place.

(3) Military Order. Military suspects may be ordered by their Commanding Officer or a senior in the military chain of command to appear in a lineup.

m. Results of Lineup Reporting. The agent in charge of the lineup will report the results of the lineup in an Investigative Action (IA). The names and addresses (command) of all lineup participants should be included. Any suggestions or objections made by the defense attorney or the suspect should be noted, as should all words of identification used by the viewing witness in making the identification. The roles of all agents participating in the lineup should also be reported. A separate witness for each witness is not required. When the lineup is shown to more than one witness, the appropriate information for each witness, i.e. times of lineup, identification statements by each witness, etc., may be included in one "Investigative Action: Lineup" exhibit.

6-14.3. SINGLE SUSPECT CONFRONTATIONS.

a. General. If a suspect is apprehended or placed in temporary detention shortly after the commission of an offense, witnesses in the general area of the offense, for identification purposes, may confront him/her singly. The single suspect confrontation should take place within minutes, no more than two hours, of the offense. Although suggestive and done without the presence of counsel, the single suspect confrontation can be a lawful identification. The courts consider it reliable where the victim or witness had ample opportunity to view the suspect at the time of the crime, provided a detailed, accurate description of the suspect and the confrontation occurs within minutes of the offense. Local practice or court rules may require a reduction of the two-hour period. In apprehension situations, preference should be given to foregoing the single suspect confrontation in favor of a formal lineup. If staging a lineup will cause a substantial delay in the identification attempt thus reducing the reliability of the identification or is impracticable under the circumstances, the single suspect confrontation may be used.

b. Confrontation Procedure. Because single suspect confrontations are inherently suggestive, agents should take all reasonable steps to assure that confrontations between suspects and eyewitnesses are accomplished as fairly as possible, with a minimum of suggestiveness. These procedures may assist in reducing the suggestiveness of a single-suspect confrontation:

(1) Circumstances of Viewing. Agents may be able to arrange the circumstances of viewing to reduce suggestiveness. For example, the suspect may be positioned with several agents who are not known to the witnesses.

(2) Informing Witness of Status of Investigation. Agents should avoid telling witnesses about the status of the investigation or the details of the apprehension of the suspect. The witness merely should be informed that a person who fits the description of the suspect has been detained for investigation.

(3) Questioning Witnesses. Agents should question witnesses so as to avoid suggesting that the person stopped has been arrested or is the perpetrator of the offense. For example, "Is this the person?" is preferable to "This is the person, isn't it?"

(4) Commenting on Validity of Identification. Agents should not comment on the validity of an identification made by a witness during a single suspect confrontation.

c. Place of Confrontation.

(1) After Apprehension/Arrest. If a suspect found in the general vicinity of the offense shortly after its commission is arrested/apprehended, the confrontation may take place either at the place of arrest/apprehension, the scene of the offense, or any appropriate place.

(2) During Temporary Detention. If a person found in the general vicinity of a crime shortly after its commission is placed in temporary detention, the confrontation should take place at the location of the stop, assuming suitable lighting and safety conditions exist. Unless special circumstances exist or the suspect voluntarily consents, the suspect should not be transported to the scene of the offense or to another location for viewing.

d. Multiple Witnesses. If there are several witnesses to the offense, consideration should be given to only one or two separately viewing the single suspect. If the suspect is taken into custody, a lineup may be arranged for the witnesses who did not view the suspect in the confrontation.

e. Right to Counsel. A suspect who appears in a single-suspect confrontation has no right to be represented by counsel at the confrontation. It is not necessary for any suspect to execute a lineup waiver during a single suspect confrontation.

f. If a line-up is contemplated after preferral or confinement, the regular line-up procedures would be followed.

6-14.4. PHOTOGRAPHIC IDENTIFICATION.

a. General. Courts have held that photographic identifications are not lineups. Therefore, a suspect has no right to counsel during the display of photographs to witnesses. Pictures displayed to witnesses can be made available to the trial court at the time of trial. Any possible unfairness could be detected through cross-examination at that time.

b. Suggested Photographic Identification Procedures. The display of photographs should not be impermissibly suggestive. These techniques are provided to assist in that regard:

(1) Number of Photographs. Select a minimum of six photographs, none of which duplicate the others.

(2) Display of Photographs. Arrange the photographs so as to leave only the face visible and to block out any identification numbers or letters which suggest prior arrest/apprehension (as in booking photos).

(3) Similarity of Photographs. Attempt to obtain photographs of persons who resemble each other in terms of physical and racial characteristics as much as possible. The photo print of the suspect should not be dissimilar to the other prints.

(4) Multiple Witnesses. Display the groups of photographs to one witness at a time. Ask each witness not to discuss his or her identification of the suspect with the other witnesses.

(5) Comments by Agents. Agents should not indicate in any manner which photograph is that of the suspect or comment on the status of the investigation or the validity of the identification.

c. Results of Photographic Identification. A written record of photographic displays, for the purpose of identifying a suspect, should be made and attached to the Report of Investigation reporting the photographic lineup. Except where wholly impracticable, the record should include the following:

(1) Record of Photographs - All photographs shown to any witnesses for the purpose of identifying a suspect should be made a matter of record. This is done by making a photographic (or superior xerographic) copy of the lineup photographs and appending copies to the appropriate Reports of Investigation. In the event identification is made, the original lineup photographs should also be entered into the evidence custody system.

(2) Identity of Persons Depicted. Identifying information on persons represented in each photograph should be maintained, if known.

(3) Marks or Scratches. The presence of any marks, scratches, folds, writings, or other notable physical characteristics on the photographs should be recorded.

(4) Date, Time and Location of Display. The date, time, and location of each photographic display should be recorded.

(5) Identity of Witness. The name and address of the witness to whom the photographs were displayed should be noted.

(6) Identity of Agent. The name of the agent who observed or participated in the photo display should be recorded.

(7) Statement. A signed, sworn statement should be taken from each witness who makes a positive identification in a photographic lineup.

d. Photographing Juveniles. The Juvenile Delinquency Act does not bar juveniles from being photographed or fingerprinted providing the files are safeguarded from disclosure. The following rules apply to the disclosure of these records:

(1) Fingerprints and photographs of juveniles who are prosecuted as adults shall be made available in the manner applicable to adults.

(2) Unless a juvenile who is taken into custody is prosecuted as an adult, neither the name nor the picture of the juvenile shall be made public in connection with a juvenile delinquency proceeding.

(3) Fingerprints and photographs of juveniles who are not prosecuted as adults shall be made available only in the following inquiry circumstances:

(a) A court of law,

(b) An agency preparing a persistence report for a court,

(c) Law enforcement agencies where the request for information is related to the investigation of a crime or a position with that agency,

(d) The Director of a treatment agency or the Director of a facility to which a court has committed the juvenile,

(e) An agency considering the person for a position immediately and directly affecting the national security, and

(f) Any victim of such juvenile delinquency; if the victim is deceased, from the immediate family of such victim, related to the final disposition of such juvenile by the court.

6-14.5. REPORTING REQUIREMENTS.

a. Exhibits. When a lineup is held, an Investigative Action (IA) form shall be made an exhibit to the ROI. When a lineup suspect who has the right to counsel waives that right, a copy of the Lineup - Acknowledgement and Waiver of Rights Form shall be made an enclosure to the (IA).

b. Reporting the Lineup in the ROI. It is sufficient to report the date and place of the lineup and the results of the lineup stated in terms of a positive, indeterminate, or negative identification of the suspect by the viewing witness. The attached IA shall contain pertinent details of the lineup.

c. Reporting the Single-Suspect Confrontation. The results of a single suspect confrontation shall be reported in detail, utilizing an Investigative Action: Single-Suspect Confrontation.

d. Reporting Suspect Identification by Use of Photograph. Attempts to establish the identity of a logical suspect by displaying photographs to a witness shall be reported in detail in the ROI, utilizing an (IA): Photographic Identification.

6-15. ASSISTANCE TO U.S. AGENCIES AND FOREIGN GOVERNMENT ABROAD

(b)(7)(E)

6-15.2. This section addresses several kinds of investigative activities, which NCIS can continue to perform, as well as those, which cannot be justified under constraints of DOD Directive 5200.27.

a. NCIS components may continue to respond to valid requests for investigative assistance in areas abroad where NCIS investigative resources are located, when the basis for request from the other Federal agency (FBI, OPM, ICE, DEA, DSS, etc.) is an authorized personnel security investigation for that agency, or (b)(7)(E). or criminal matter under the investigative jurisdiction of the other agency. Under these circumstances, NCIS can continue to furnish other U.S. agencies with the results of NCIS file checks, including the DCII (consistent with Privacy Act declarations for routine uses), and (b)(7)(E) and criminal information collected or made available from other agencies concerning such matters as terrorism, drug trafficking, black-marketing, customs violations, espionage and other serious counterintelligence or criminal cases. Without attempting to catalog all authorized investigative assistance, NCIS may also perform

additional activities concerning non-DOD affiliated U.S. citizens abroad, when requested by competent authority, as illustrated by the following:

(1) Assist in the location, but not the arrest, of U.S. persons abroad who are Federal fugitives.

(2) Furnish information to the U.S. Secret Service regarding individuals and organizations that pose a possible threat to officials for whom the Secret Service has protective responsibility.

(3) Provide information regarding the movement of ships and vessels suspected of involvement in illegal activity.

(4) Locate and interview individuals abroad who are witnesses or suspects in investigations being conducted by other Federal, State, or local law enforcement agencies in the U.S.

(5) Provide forensic laboratory support or other technical, logistic or administrative assistance on a case-by-case basis when permitted under the Economy Act, and not otherwise prohibited by law.

b. While NCIS is permitted under the language of the preceding paragraph to continue to perform a wide range of investigative tasks abroad for other Federal agencies in the interests of economy, it is essential that NCIS components not accumulate non-criminal investigative records on persons not affiliated with the DOD in the process.

c. DOD Regulation 5240.1-R, Procedures Governing The Activities Of Dod Intelligence Components that Affect United States Persons states that "assistance may be rendered to law enforcement agencies and security services of foreign governments or international organizations in accordance with establishment policy and applicable status of forces agreements; provided that DOD intelligence components may not request or participate in activities of such agencies undertaken against United States persons that would not be permitted such components under these procedures."

(1) In the application of this policy, it would be improper for NCIS components to obtain and pass on to foreign governments information relating to the manner in which non-DOD affiliated U.S. individuals exercise their First Amendment rights.

(2) At the same time, the general rule cited above will not prevent a number of exchanges of information that NCIS may validly acquire and retain relating to U.S. citizens abroad, as illustrated by these examples:

(a) Information relating to the present or former military or civilian employee status of U.S. citizens abroad or information relating to their true identity may be disclosed. Requests regarding personnel presently or formerly involved in U.S. intelligence activities should not be honored but discreetly referred to the appropriate U.S. agency.

(b) Information relating to the involvement of U.S. citizens in criminal activities abroad. Such acts may include black-marketing, drug trafficking, theft of arms and ammunition from U.S. facilities, crimes against the U.S. government, espionage, sabotage, international terrorist activities and similar acts of a criminal nature.

(c) Forensic laboratory support and field tests of narcotics or other controlled substances.

(3) When a host government requests information of a non-criminal nature regarding a non-DOD affiliated "U.S. Person" residing abroad or in the U.S., the following procedures will be followed: The NCISFO will direct the request to the appropriate operational department at NCISHQ (either Code 22 or 23), setting forth the request and providing as much justification for honoring the host government's request as possible. If approved at NCISHQ, NCIS personnel will gather the information through investigative efforts, primarily through liaison or coordination with other investigative/governmental agencies as appropriate. The information will then be transmitted back to the requesting component and a copy to the NCISFO with specific guidelines as to the use, which may be made of the information provided. Such requests will be handled in a most expeditious manner at NCISHQ. These procedures are necessary in order to assure compliance with the spirit and intent of policy and guidelines provided in DOD Directive 5200.27 and DOD Regulation 5240.1-R.

(4) Obviously, all situations requiring the rendering of NCIS assistance to other U.S. agencies and foreign governments cannot be addressed in this section. There will be unanticipated circumstances arising, which should be referred to NCISHQ (000L, 0022, or 0023) for resolution.

6-16. ADJUDICATIVE REFERRALS

6-16.1. Implicit within its responsibility to conduct investigations of major criminal offenses is the responsibility for NCIS to ensure results of successfully completed investigations are presented to the appropriate adjudicative authority or agency and that actions or decisions resulting from such presentations are documented. This pertains to all investigations initiated and conducted by NCIS under case categories 3 through 8, which develop a suspect with the exception of certain subcategories of investigation utilized to report information of a counterintelligence nature (i.e., subcategories 3D, 3E, 3G, 5C, 5G, 5M, 5S, and 5T). Furthermore, since a prosecutable case has been presented, the investigation will not be closed until disposition has been reported for all titled subjects, co-subjects and corporate subjects via ROI via appropriate DONCJIS entries.

6-16.2. Resolved criminal investigations with military personnel identified as subjects or co-subjects will be briefed to the military commander who has disciplinary responsibility for the individuals; this briefing will be documented in a ROI (INTERIM). The documentation will include the name, position, organization and response of the person briefed and the date of the briefing. Merely listing the commands which have

disciplinary responsibility for the individuals as "INFO" addressees under the distribution caption on a ROI (INTERIM) that provides case summary or Prosecutive Summary does not satisfy the prosecutive referral requirement. In those resolved investigations identifying civilians, corporations or companies as suspects, similar documentation of the prosecutive referral is required.

6-16.3. Referral of investigations to the Department of Justice of crimes involving Classified or Sensitive programs will be affected without prior coordination or referral to the local United States Attorney.

6-17. DECLINATION OF PROSECUTION BY DEPARTMENT OF JUSTICE/UNITED STATES ATTORNEY

6-17.1. The policy set forth in this section is published as directed by the Department of Defense Inspector General Criminal Investigations Policy Memorandum Number 2.

6-17.2. In all cases investigated by a DOD criminal investigative organization, including joint investigations with other investigative organizations, where Federal prosecution has been declined by DOJ; DOD criminal investigators should ensure that prosecutive declinations by DOJ are memorialized in a manner that encourages, when appropriate, other criminal, civil, contractual or administrative remedies.

6-17.3. Where it is the practice or intent of a United States Attorney's Office or other DOJ component to issue a written declination, DOD criminal investigators shall seek the inclusion of statements similar to those listed below, when appropriate:

a. Declinations where prosecution standards were not met: "The facts evidence a degree of criminal misconduct on the part of (subject(s)). However, the case does not meet the United States Attorney's standards required for Federal prosecution. This declination should not be construed by your agency or command in such a way as to preclude consideration of other available criminal, civil, contractual and administrative remedies. As the victim of the alleged offense(s), it appears appropriate for your agency or command to consider initiating other available remedies. These remedies should be discussed with the civilian or military attorneys assigned to your agency or command."

b. Other Declinations: "The facts as developed to date do not merit criminal prosecution against (subject(s)) by this office because [sic]. This declination should not be construed by your agency or command in such a way as to preclude consideration of civil, contractual, and administrative remedies. The facts are sufficient to warrant consideration of these other available remedies, and they should be discussed with the civilian or military attorneys assigned to your agency or command."

6-17.4. Where it is not the practice or intent of a United States Attorney's Office or other DOJ component to issue a written declination, DOD criminal investigators shall consult with the prosecutor issuing the declination to obtain approval in including in the

investigative report, when appropriate, a statement similar to those listed in paragraph NCIS-6, Chapter 19.

6-17.5. The specific written statement of the United States Attorney's Office or other DOJ component or the investigator's memorandum required in NCIS-6, Chapter 21, will be obtained in those investigations where the United States Attorney declines prosecution and the subject is one or more of the following:

a. Federal employee, either military or civilian;

b. Individual, company or business entity attempting to do or doing business with the DOD;

c. Employee of an individual, company or business entity attempting to do or doing business with the DOD;

d. Individual, company or business entity (or its employees) acting on behalf of an individual, company or business entity attempting to do or doing business with the DOD;

e. Prime contractor, subcontractor at any tier or independent contractor that submits offers for, is awarded, or may be expected to submit offers for or be awarded a DOD contract or subcontract; or conducts business with the DOD as an agent or representative of another contractor.

6-17.6. The assigned investigator should be prepared to assist the prosecutor in preparing the specific written statement. This may include the preparation of a draft statement, if so directed by the prosecutor. A copy of the prosecutor's specific written statement or the investigator's memorandum will be included in any interim and final reports of investigation as an exhibit to the prosecutive status section.

6-18. DETAILS AND DISPOSITION INVESTIGATIONS

6-18.1. The case category relative to the offense for which the suspect was arrested will be utilized for all investigations initiated for the sole purpose of obtaining details and/or dispositions of current civil arrests. The ROI (OPEN) should be specific in stating the coverage requested by command. The ROI (OPEN) CCN case project code for a request from a Navy or Marine Corps command will be NA for Navy or MA for Marine Corps. The investigation should include obtaining copies of police reports if available or interviews of arresting officers if necessary. If details and disposition are requested, this must be noted. If disposition is requested, attempts should be made to obtain copies of the court or prosecuting attorney's disposition document. A details and disposition investigation will not be initiated to pursue information surfaced during the course of an ongoing criminal investigation.

6-18.2. In some cases, the command will not need the disposition and no attempt should be made to obtain it except in cases involving serious felony offenses having obvious Naval Military Personnel Command or other SOG interest. In those cases when a command does request disposition the case must be left open until the court action is completed and the disposition is obtained. If the command has other means of obtaining disposition, such as a command representative at judicial proceedings or arrangements are made with the arresting authorities for a Navy detainee and notification of the Navy of the disposition, this information should be reported and a closing ROI may be written.

6-18.3. If additional investigation is appropriate after appraisal of the command of the details and disposition of the civil arrest, such as interrogation of suspects, interviews of corroborating witnesses, or investigation essential for the proper administrative or judicial disposition by the command; then the project code identifier must be changed from NA or MA. It is NCIS policy to ensure all logical investigation is conducted so that Naval authorities can take appropriate action.

6-18.4. If at the time of the initial request for details and disposition of the civil arrest the command desires additional investigative assistance, i.e., interrogation of suspects, etc., then a standard criminal investigation should be initiated. This may occur because no civil charges will be preferred, the charges have been dismissed, or the civil investigation has not been brought to a logical conclusion and the subject is not going to be prosecuted by civil authorities. However, if only details and disposition are requested, then a details and disposition investigation will be initiated regardless of the date of the arrest or the status of the investigation or judicial proceedings.

6-18.5. In those instances where there are multiple types of criminal offenses and a criminal vice details and disposition investigation is required, the criminal category used should be for the most serious offenses as determined by the table of maximum punishments contained in the Manual for Courts-Martial.

6-18.6. Investigative resources might be conserved through the increased use of the National Law Enforcement Telecommunications System (NLETS) for obtaining details and disposition of arrests in criminal investigations. Depending on a number of variables below, this alternative to sending an agent to personally check a record could be an effective timesaver.

6-18.7. Detailed guidance concerning the use of NLETS for record checks can be found on the NCIS Info-Web page at http://infoweb.ncis.navy.mil/ under NLETS User's Guide. It should be noted that details and disposition investigations are considered to be for criminal purposes vice employment and the NLETS Inquiry purpose code PUR/C should be utilized. This greatly increases the chances an agency will respond to an inquiry. Basically, a records check inquiry to law enforcement agency via NLETS is an administrative message which the agency may or may not choose to answer. Although a NLETS message will receive more prompt attention than a letter, responses will vary from agency to agency. Additionally, the response will most frequently confirm the arrest and provide only a brief

summary of the details. For this reason, it may be best to request a mailed copy of the arrest report.

6-18.8. The use of NLETS in details and disposition investigations is encouraged; however, the extent of utilization is left to the discretion of individual offices. Leads to check agencies outside a NCISFO's area of responsibility should continue to be disseminated to the servicing NCISRA leaving the NLETS decision to that office.

6-18.9. Care should be taken to ensure that details and disposition investigations are not initiated to obtain information in lieu of or to supplement a personnel security investigation (PSI). PSI(s) regarding Department of Navy (DON) personnel are the sole responsibility of the Defense Security Service (DSS) or the Office or Personnel Management (OPM). Should a PSI be found to be incomplete or necessary to prove or disprove subsequent allegations primarily to establish an individual's continuing suitability for a security clearance or trustworthiness for certain assignments, DIS will open a special investigative inquiry upon request. NCIS activities will not normally expend investigative resources in conducting PSI(s) or post adjudicative inquiries in matters relating primarily to clearance suitability or trustworthiness matters.

6-19. FINGERPRINTING OF SUSPECTS

6-19.1. DoD Instruction 5505.11, Fingerprint Card and Final Disposition Report Submission Requirements of December 1, 1998 (revised 20 June 2006) directed all DOD Criminal Investigative Organizations (DCIOs) and DOD Law Enforcement Agencies to submit criminal history data to the FBI, Criminal Justice Information Center (CJIS) in Clarksburg, WV. The DoD Instruction is found at the following Web site: http://www.dtic.mil/whs/directives/corres/html/550511.htm .

6-19.2. The criminal history record that is posted on the NCIC is created by the receipt and acceptance by the FBI of the FD-249, Criminal Fingerprint Card. The record is completed when the Final Disposition (Green form) is reported. Offender criminal history records required under this policy will be initiated by preparation and submission of FBI Form FD-249 (REV 6-11-99), criminal fingerprint card, to NCISHQ Code 24B3.

6-19.3. The policy of the NCIS is to obtain at least two inked ten-print cards of the suspect at the time of interrogation for an offense or offenses. The card must be completed in accordance with the instructions and be typed or clearly printed. Fingerprints obtained during the interrogation process are maintained in the investigative case file until command initiates judicial or non-judicial action.

6-19.4. Requirement for submission of criminal fingerprints pertains to all military service members, as well as, civilian subjects investigated for commission of an offense listed in DODI 5505.11, or any offense under the Federal Assimilative Crimes Act (18 USC 13), which has a maximum punishment of more than one year confinement, and, who are the subjects of any resultant judicial or non-judicial military proceeding. A military “judicial proceeding” is a court-martial (i.e. general, special, or summary court

martial) pursuant to an Article 32, UCMJ. A "non-judicial proceeding" is conducted in accordance with Article 15, UCMJ.

6-19.5. When judicial or non-judicial action is initiated by command, submit two fully completed form FD-249 (REV 6-11-99), criminal fingerprint cards by certified mail to NCISHQ, Code 24B3, 716 Sicard Street Suite 2000, Washington Navy Yard DC 20388-53880. Mug shot photographs that are mailed with the original criminal fingerprint cards will be included in the package sent by Code 24B3 to the FBI/CJIS.

6-19.6. In the ROI (ACTION) list CODE 24B3 in the ACTION line, with no response required to this tasking. Additionally, the certified mail number will be maintained by the submitting unit or field office in order to track submissions. Fingerprint cards and any associated mug shots are not to be enclosed as exhibits.

6-19.7. The current revised DoD instruction specifically addresses policy requirements for the submission of fingerprint cards and criminal history data for both military service members, and civilian subjects of DCIO investigations. NCIS will be responsible for the taking and submission of fingerprints and reporting final disposition.

6-19.8. At the conclusion of the judicial or non-judicial military proceeding, the control agent/NCISRA will report disposition (green form) information by means of the FBI form R-84, Final Disposition Report, completed in accordance with form instructions, which is sent directly to: Assistant Director, Criminal Justice Information Services, POB 4142, Clarksburg WV 26302-9922, using the postage free, preaddressed envelope provided by the FBI. The final disposition information will be filed on the record FD-249, criminal fingerprint cards, in lieu of the R-84, Final Disposition Report, if the disposition is known at the time of the submission of the fingerprints.

NOTE: It is critical that the FBI number, which is established specifically for an individual, be obtained and entered onto the R-84 form prior to its submission. Absence this assigned number on the R-84 form, the FBI will be unable to match the final disposition information to the correct criminal history record. This can be accomplished by running an Interstate Identification Index (III) query commonly referred to as a "Triple I" query. Enter this FBI number onto the R-84, prior to its submission.

6-19.9. CIS policy is to obtain disposition information from the command having disciplinary authority over the suspect for each suspect charged as the result of an NCIS investigation. The control agent/NCISRA will report the disposition information in the CLOSED ROI.

6-19.10. The NCISHQ supply department will provide, at no cost, the FBI form FD-249, Criminal Fingerprint Card, the FBI form R84, Final Disposition Report, and the FBI/CJIS postage free, preaddressed envelopes for mailing of the R-84, Final Disposition Report.

6-20. VICTIM AND WITNESS ASSISTANCE PROGRAM (VWAP)

6-20.1. The principal justification for standards relating to the proper treatment of victims and witnesses is that they are integral to sound law enforcement practices. Compliance with those standards can enhance NCIS's ability to conduct investigations, which survive to plea or trial. Research findings over time and across jurisdictions consistently indicate that a major cause for case attrition before plea or trial is witness-related problems. Similarly, research indicates that the probability of conviction increases markedly as the number of cooperative witnesses increases. If victims and other witnesses are subjected to what they consider poor treatment, they can be expected to offer something less than total cooperation with law enforcement agencies. This can have a devastating impact on investigations and subsequent prosecutions. If they are treated with sensitivity to their victimization, they are more likely to testify against the suspect.

6-20.2. The Victims' Rights and Restitution Act of 1990 (VRRA) established the Crime Victims' Bill of Rights, as set forth below:

a. The right to be treated with fairness and with respect for the victim's dignity and privacy.

b. The right to be reasonably protected from the accused offender.

c. The right to be notified of court proceedings; the right to be present at all public court proceedings related to the offense, unless the court determines that testimony by the victim would be materially affected if the victim heard other testimony at trial.

e. The right to confer with attorney for the government in the case.

f. The right to restitution.

g. The right to information about the conviction, sentencing, imprisonment, and release of the offender.

6-20.3. Victims of crime will be treated with compassion, respect, and dignity at all times, and must be informed of certain information during the course of the investigation and prosecution of the crime, if requested. Overseas, these services pertain only to active duty and civilian employees and their families.

6-20.4. The Victim/Witness Program consists of four principal areas: the base police or patrol element, the NCIS/CID or investigative element, the NLSO/SJA or trial element, and the brig/prisons or corrections element. Inextricably linked to these four are medical, counseling, and religious personnel. The following is a summary of the responsibilities of NCIS Special Agents in dealing with victims and witnesses of crime:

a. Determine ahead of time the information that will be used in the blank spaces of the DD Form 2701 informational brochure and routinely carry brochures.

b. Ensure that victims and witnesses are informed of available emergency, medical and social services and how to obtain these services, if needed.

c. Provide information on restitution and compensation to which the victim may be entitled. It is NCISHQ's understanding that victims of crime overseas on military bases may be eligible for compensation through the state Crime Victims' Compensation Office in their home states, depending on individual state law. A copy of the current crime victim compensation program contact list, which provides the principal point of contact for each state, should be available in the base legal office or the NLSO. If not, the information will be available through NCISHQ. A list of benefits, which may be covered by compensation, is in 6-20.5, below.

d. Provide information on victim counseling and treatment programs which may be available within the local community or from base services, and assistance in making contact with those services, if needed.

e. Explain the role of the victim in a criminal investigation and prosecution and what may be expected from the system and victims and witnesses. This should not be a detailed presentation on the criminal justice system, but a general idea of how the investigation will be handled and an overview of the prosecutive process. Should a suspect be identified, the trial counsel will provide more detailed information on prosecution.

f. Special Agents should arrange for victims and witnesses to receive reasonable protection from suspected offenders and persons acting in concert with or at the request of the offender. NCIS cannot guarantee safety but can help the victim determine steps to be taken which will minimize the possibility of further harm from an offender.

g. If the victim(s) so requests, the case agent or other NCISFORA personnel should keep the victim(s) informed of the status of the investigation as long as such information does not interfere with the investigation itself.

h. Victim(s) and witness(s) should be informed of the apprehension/arrest of a suspect.

i. The responsibility of informing the victims and witnesses of the filing of charges against an accused, all court appearances, and the release or detention of an accused pending action generally falls upon the trial counsel; however, it can occasionally be left to the case agent.

j. The law further requires the reasonable separation of victims and witnesses from the accused during the trial. Efforts should also be made within NCIS offices to keep victims and witnesses separate from any suspect during the investigation.

k. Special Agents should ensure that any property of the victim being held for evidentiary purposes is maintained in good condition and returned to the victim as soon as it

is no longer needed. This is specifically mentioned in the Victims' Rights and Restitution Act of 1990.

l. Special Agents should ensure that the cost of medical examinations of sexual assault victims conducted for evidentiary purposes will not be borne by the victim. The VRRA requires the investigative agency to pay for the exam or to reimburse the victim for the cost of the exam (if it cannot be done on a no-fee basis, such as in a military medical facility).

m. Special agents conducting interviews of victims and witnesses should annotate their case notes in some manner to document their provision of crime victim assistance information to that person.

6-20.5. To expand the information provided above regarding crime victim compensation, the following is provided. Generally, compensation is provided by the state in which the crime occurred and is limited to any of the following, which are not otherwise, covered by insurance:

a. Medical or hospital bills;

b. Mental health counseling;

c. Actual loss of earnings due to crime-related injuries;

d. Loss of support for dependents of victims who are deceased or disabled as a result of crime;

e. Funeral and burial expenses;

f. Loss or damage to eyeglasses, hearing aids, or other medically necessary devices; and

g. In a few states, awards for pain and suffering.

6-20.6. To expand the information provided above regarding protection of victims, the following is provided. Besides the availability of a military protection order or a civilian temporary restraining order available to the victim, Title 18 USC provides for fines and imprisonment for assault and battery on witnesses. Section 1512 provides for a $250,000 fine and 10 years imprisonment for anyone who knowingly uses intimidation or physical force (including threats) with the intent to influence the testimony of any person or to cause a witness to withhold testimony, alter/ destroy evidence, etc. Section 1513 provides for a $250,000 fine and 10 years imprisonment for anyone who causes, or threatens to cause, bodily injury or property damage in retaliation against a witness, victim, or informant. Section 3579 allows a court to order restitution to the victim when sentencing a defendant convicted of any offense under Title 18 USC. Restitution is not available through military court martial sentencing except through a pre-trial agreement.

6-20.7. Besides the normal definition of victim of crime, in the case of a victim who is under 18 years of age, incompetent, incapacitated, or deceased, one of the following (in order of preference) should be kept informed as if it were the victim:

a. Spouse

b. Guardian

c. Parent

d. Child

e. Sibling

f. Another family member

g. A person designated by a court of law

6-20.8. In deciding which witnesses should be afforded victim/witness services, the following discussion is provided. At one end of the scale is the eyewitness to a violent crime, who has direct knowledge of what happened to the victim. Obviously, such a witness should be afforded full victim/witness services and given considerable care by the Special Agent or the victim/witness coordinator. At the other end of the scale is the disbursing clerk who provides access to pay records of a suspect. Such a witness would normally not be provided any victim/witness services. As Special Agents, NCIS must all be watchful and aware of the depth of involvement in the incident a particular witness may have had and how much the incident affected that witness. Eyewitnesses to violent crimes should routinely be provided the same information afforded the victim. As witnesses become farther and farther removed from the actual incident itself, the need to provide victim/witness services diminishes. Defense witnesses and individuals involved in the crime as perpetrators or accomplices are not eligible for these services.

6-20.9. Victim and witness laws require much of the criminal justice system. After the investigative phase is over, the trial phase and the corrections phase follow. It is important for the victim/witness coordinator in each of those elements to know how to contact victims and witnesses in order to determine if they desire continuing information on the status of the offender through the trial process and, later, during any period of incarceration awarded by the court. Since NCIS Special Agents play such a significant role in the initial dealings with victims and witnesses, it is incumbent on Special Agents to ensure that re-contact data is obtained from victims and key witnesses. Addresses and home phone numbers of these victims and witnesses should never be published in an ROI, but should be available to pass to the trial counsel and/or corrections personnel as needed. It is recommended that a list of contact data for victims and appropriate witnesses be maintained in the case file in an easy-to-find location so that other NCIS personnel seeking that information in the absence of the

case agent will know where to look, such as on a separate sheet of paper on the left side of the case file.

6-20.10. There is a transition area where the responsibilities of NCIS end and the responsibilities of the trial counsel begin. This is not a sharp line, but an area in which, if a suspect has been identified, the Special Agent and the trial counsel should be in close coordination to ensure that victims and appropriate witnesses are kept informed.

6-20.11. Enclosure (3) to DoD Instruction1030.2 is DD Form 2701, the brochure entitled Initial Information for Victims and Witnesses of Crime, an informational brochure which is to be used by all special agents and other NCIS personnel, as appropriate, to inform victims and witnesses of crime of certain rights and points of contact within the criminal justice and victim/witness support systems. The blanks on the back of the brochures should be filled in by the case agent or other responding agent, as appropriate, and given to all victims of crime investigated by NCIS. If jurisdiction resides with another agency and that agency has provided victims with similar information, then. Of course, the case agent must be sensitive to the needs of the victim and provide those victims with a copy of the brochure whenever, in the judgment of the Special Agent, it may be in the best interest of the victim or witness to do so.

6-20.12. Each field office shall assign one person as the Field Office Victim and Witness Assistance Coordinator (VWAC). This person may be either a special agent or support person but should be someone genuinely interested in the VWAP and able to communicate and coordinate effectively with the agent corps as well as with victim/witness coordinators at counterpart agencies. The Field Office VWAC's primary responsibility is to ensure all personnel within the field office understand the VWAP and their responsibilities toward victims and certain witnesses within NCIS jurisdiction. VWACs may have direct contact with victims and witnesses, but that responsibility is primarily that of the case agent. VWACs should provide annual training on the VWAP to each resident agency within the field office and will serve as the primary point of contact for questions about the VWAP from field office personnel. The name of the field office VWAC should be provided to the NCISHQ VWAP Program Manager to ensure the smooth flow of information on evolving victim/witness issues occurs.

6-20.13. Each SAC, ASAC, or SSA should make contact with the NLSO or SJA aboard base to ensure the handoff from NCIS to trial counsel is properly coordinated vis-à-vis victim and witness services. This may be best performed through participation in the command Victim/Witness Council. Ensure that commands are aware of any personnel within the command who become victims of crime.

6-20.14. When using victim preference statement (VPS) form, a ROI (ACTION) should be used as the means to report such an event. The VPS is not designated “For use” by trial counsel when a victim declines to cooperate in any judicial proceedings. If the victim does decide to execute the VPS form or otherwise decline to participate in the investigation, NCIS policy requires that all viable leads be exhausted prior to closing the investigation.

6-20.15. The VPS forms should only be used for victims of sexual assault (rape, indecent assault or other sexually motivated criminal offenses). In cases where the victim is a juvenile, a parent or guardian should not be permitted to sign a VPS on behalf of the child victim. In those instances, an ROI should be used to document the parent/guardian's preferences and the investigation should proceed accordingly.

6-20.16. When responding to a complaint of rape or sexual assault, the agent may find that the victim does not want to cooperate in the investigation, sometimes for a variety of reasons.

a. In an understanding manner, the agent should explain to the victim the possible consequences of not cooperating, e.g. someone else being victimized by the suspect. Every reasonable effort should be made to encourage the victim to pursue the matter. The victim will still be advised of information regarding his/her rights as a crime victim.

b. The case agent will review the facts of the investigation with his/her supervisor and a determination will be made as to whether to present the victim with a VPS form. If the decision is made to do so, then the victim should be approached the following day and presented with the form provided at the end of this chapter. Contacting the victim the next day will allow the victim time to reconsider his/her decision not to participate in the investigation and prosecution. The victim should be informed that his/her signature on the VPS does not preclude additional investigative efforts to resolve the matter and it does not preclude the command from taking action. If the victim declines to cooperate and declines to sign the VPS, ROI (IA) detailing the attempted interview will be prepared.

c. Use of the VPS and guidance on continuing investigative action can be summarized as follows:

(1) The agent shall not discuss the existence of the VPS prior to the victim expressly stating a desire not to participate in the investigation.

(2) The VPS may only be used with the concurrence of a supervisor and be documented in the SSD that the supervisor concurred.

(3) The VPS will not be used during the initial interview with the victim unless the victim specifically requests no further contact with NCIS.

(4) The VPS will not be used with a victim until the victim has had an opportunity to consult with a victim advocate.

d. The VPS will not be used in cases where a victim was initially cooperative and later changed his/her mind during the pendency of the investigation. An ROI (INTERIM) will document such a decision at that time. An investigation will be

conducted even without the victim's cooperation if viable leads exist or if sufficient information is available.

e. The ROI (INFO) will be used to document those cases where the victim declines to cooperate and no viable leads exist or there is insufficient information to pursue an investigation. This ROI (INFO) will document that the agent's supervisor affirms that no viable leads exist which would warrant further inquiry into the matter. In responding to a sexual assault complaint and encountering a victim who does not want to provide information about the incident, special agents should make every effort to explore the concerns of the victim and encourage his/her participation in the investigative process. Special Agents are reminded that whether cooperating or not, the individual is still regarded as a victim and should be treated as such.

6-20.17. All NCIS offices should have the current VPS form (1998). Any other forms should be destroyed. Any questions regarding the use of the VPS and the ROI (INFO) will be directed to Code 0023.

6-21. HATE CRIMES

6-21.1. DEFINITION.

a. A hate crime is a criminal offense that is motivated by the perpetrator's bias against the victim's race, color, religion, or national origin. Although the term "hate crime" is frequently used, the statute prohibiting them, 18 USC 245, provides a very narrow interpretation of what qualifies as a hate crime. Also, prosecution of a hate crime requires approval from the Attorney General, the Deputy Attorney General, the Associate Attorney General, or an Assistant Attorney General designated by the Attorney General to act in this capacity.

b. The UCMJ does not contain a prohibition on hate crimes per se. Within the DON, U.S. Navy Regulation 1167 prohibits supremacist activities that are commonly associated with hate crimes. NCIS does not normally investigative hate crimes as a separate, distinct offense under the UCMJ. Allegations of hate crimes should be investigated in accordance with recognized procedures for investigating the underlying or primary crime, i.e. assault, rape, homicide, housebreaking, etc. In addition to any other criminal charges stemming from an investigation, the convening authority could charge a suspect with violation of Article 92 of the UCMJ, failure to obey an order or regulation (U.S. Navy Regulation 1167), if evidence of supremacist activities or views are found during the investigation.

c. The Regulations of Courts Martial 1001 (b)(4) allows the presentation of evidence that the offender selected the victim bases on "actual or perceived race, color, religion, national origin, ethnicity, gender, disability, or sexual orientation" during the pre-sentencing portion of a court-martial.

6-21.2. ELEMENTS OF A HATE CRIME.

a. The key element of a hate crime requires the offender's bias to be the motivation behind the criminal act. Issues to consider when determining whether an underlying crime can be associated with a hate crime are:

(1) The offender and victim were of different race, religion, disability, sexual orientation, and/or ethnicity/national origin; or

(2) Bias-related oral comments, written statement or gestures were made by the offender, which indicate his bias; or

(3) Bias-related drawings, markings, symbol, or graffiti were left at the crime scene; or

(4) Certain objects, items or things that indicate bias were used; or

(5) The victim is a member or advocate of a racial, religious, disability, sexual orientation, or ethnic/national origin group; or

(6) The offender was previously involved in a similar hate crime or is a hate group member; or

(7) The area where the crime occurred is a known locale of high tensions between groups with a historically established animosity toward each other; or

(8) Several incidents occurred in the same locality, at or about the same time and the victims were all of the same race, religion, disability, sexual orientation, or ethnicity/national origin; or

(9) The victim was engaged in activities promoting his race, religion, disability, sexual orientation, or ethnicity/national origin; or

(10) The incident coincided with a holiday or a date of particular significance relating to a race, religion, disability, sexual orientation, or ethnicity/national origin: or

(11) There are other indications that a hate group was involved (i.e., claimed responsibility).

6-21.3. INVESTIGATIVE PROCEDURES.

a. Almost any type of crime against a person can be classified as a hate crime if it is to be shown that the perpetrator selected the victim based on the victim's race, color, religion, or national origin. It is important to note that the mere fact the offender is biased against the victim's race, color, religion, or national origin does not constitute a hate crime. In order to be categorized as a hate crime, the offender's bias toward the victim must be the motivation behind selection of the victim.

b. Special attention should be paid to indications of involvement by members or supporters of supremacist groups or other groups that advocate violence toward persons or depriving them of their civil rights on the basis of their race, color, religion, or national origin. This can manifest itself in several ways to include: graffiti or other markings left at the crime scene, statements made by the perpetrator(s), the timing of the crime to coincide with a date of significance to either the perpetrator(s) or victim(s).

c. Investigations of allegations of a hate crime should focus on the elements of the crime for the underlying offense(s). Personnel involved in those investigations should determine the nature of the underlying offense(s) and refer to the appropriate chapter within this publication. Other investigative considerations include:

(1) Determine if there is a scene to examine.

(2) Photograph, sketch, and collect all physical evidence such as spray paint cans, graffiti, property damage, and symbolic objects, such as swastikas or the letters KKK.

(3) Photographs of graffiti consisting of racial, ethnic, religious, gender-related, or sexual orientation-related epithets should be taken immediately following the incident.

(4) If appropriate, seize the victim's clothing and footwear for possible laboratory analysis to determine if trace evidence exists, i.e., blood, salvia, glass fragments, paint/spray, clothing fibers.

(5) Seize any closed circuit television (CCTV) footage and note the presence of other CCTV. If unable to seize at the time, ensure steps are taken to preserve the footage.

6-21.4. INTERVIEW OF THE VICTIM.

a. During the interview of the victim, the case agent should be extremely sensitive to and respectful of their cultural perceptions of law enforcement or desire to conceal or deny their affiliation with the group the offender intended to harm. A determination should be made if the victim has been victimized in any prior incidents. Other issues to consider when interviewing the victim:

(1) Does the victim perceive the action of the offender to have been motivated by bias. Is there clear motivation for the crime or was the incident committed during a specific holiday of significance to the victim/offender's group.

(2) What do the demographics of the area tell you about the incident.

(3) Were the offender and victim from different backgrounds. Were biased comments, written statements or gestures made by the offender indicating bias.

(4) Were certain objects, items or things which indicate bias used, e.g. the offenders wore white sheets with hoods covering their faces, a burning cross was left in front of the victim's residence.

(5) Was the victim visiting a neighborhood where previous hate crimes were committed. Have several incidents occurred in the locality, at or about the same time and were the victims of the same background.

6-21.5. RIGHTS WARNING. There is not a specific Article 31b rights warning for suspects involved in alleged or suspected hate crimes. When suspicion exists that a hate crime has occurred, suspects should be advised of their Article 31b rights pertaining to the underlying crime(s) as well as failure to obey a regulation or order (in this case U.S. Navy Regulation 1167).

Appendix 1: Military Suspect's Acknowledgement and Waiver of Rights

Place: NCISRA Great Lakes, Il
Date: November 1, 2001

I, Wynott Frank Smith SA USN, 123-45-5678, have been advised by Special Agent John R. Straightshooter that I am suspected of setting a fire in Barracks 710, located aboard the Naval Training Center, Great Lakes, IL in violation of UCMJ Article 126, Arson.

I have also been advised that:

1) I have the right to remain silent and make no statement at all;
(2) Any statement I make can be used against me in a trial by court martial or other judicial or administrative proceeding;
(3) I have the right to consult with a lawyer prior to any questioning. This lawyer may be a civilian lawyer retained by me at no cost to the United States, a military lawyer appointed to act as my counsel at no cost to me, or both;
(4) I have the right to have my retained lawyer and/or appointed military lawyer present during this interview; and
(5) I may terminate this interview at any time, for any reason.

I understand my rights as related to me as set forth above. With that understanding, I have decided that I do not desire to remain silent, consult with a retained or appointed lawyer, or have a lawyer present at this time. I make this decision freely and voluntarily. No threats or promises have been made to me.

Signature :_____

Date & Time: _____

Witnessed: _____

_____

STATEMENT

At this time, I, Wynott Frank Smith, SA USN, 123-45-5678, desire to make the following voluntary statement. This statement is made with an understanding of my rights as set forth in the Suspect's Acknowledgement and Waiver of Rights form of November 1, 2001, 8:30 AM. It is made with no threats or promises having been extended to me.

I was born on July 19, 1988 in East Overshoe, Nevada. I am currently assigned to the Transient Personnel Unit, Naval Administrative Command, Naval Training Center, Great Lakes, Ill., and have been assigned to that Command since April 2001.

I started the fire at Barracks 710, but I did not do it to hurt anybody. I did it to get even with BM2 Sykes, one of the MAAs at the barracks. I did it because I wanted to get SYKES in trouble for leaving paint thinner in the MAA's Cleaning Gear Locker after Chief JOHNSON, the CMAA for TPU, had told him he could not leave the paint thinner there because it was a fire hazard.

On Friday October 19, 2001, I was part of a four-man working party that was painting the stairs and railings at the barracks. SYKES was in charge of the working party. When it was time to secure, we had not finished the painting. SYKES told me that I had to finish the job, and he secured the other three guys. SYKES was the duty MAA for that evening so he was staying around to make sure I finished. I went to evening chow and finally completed the job and got everything cleaned up around 1830.

I was broke, so I hung around the barracks until around 2230 that evening. At that time a guy I know, Dusty Rhodes SR, USN, came back from liberty and I borrowed $5.00 from him so I could go on liberty. I then went out to a bar on Sheridan Road in North Chicago, Ill., to have a few beers. The name of the bar was the Melody Lounge. I stayed there until closing time, around 0100. While there I watched some guys playing pool and spent my time talking to them. There were four guys playing but I don't know their names. From talking to them, I know that two of them were sailors from Machinist Mates School, and I think the other two guys were civilians. I would describe the two sailors as White, males, about 18 to 20 years old, average build and height (about 160 Ibs. and 5' 8n top 5' 9n in height), with brown hair. Both were wearing Levi-type trousers. One .wore a blue and green short-sleeve shirt with collar and buttons down the front, while the other wore the same kind of shirt, only it was orange. The one with the orange shirt was also wearing wire-rimmed glasses. One of the civilians was a Black, male, in his early 20's about 5' IOn in height, had a heavy build (about 200 to 215 Ibs.), and a light complexion. He was wearing brown trousers, a yellow T-shirt, and ankle-high brown boots. The other civilian was a White, male, in his early 20's, about 6' 3n in height, skinny build (about 150 to 160 Ibs.) and was wearing cut-off Levi shorts and a light green tank-top shirt. The two civilians seemed to know the bartender as they called him by his first name, which I think was John.

I left the Melody Lounge by myself and walked back aboard the base. While I was walking back to the barracks I started thinking about SYKES and how he has been on my back for the last couple of weeks. I remembered that Chief JOHNSON had told him about the paint thinner. I knew the paint thinner was still in the locker when I secured from the painting detail at about 1830, because I had used it to clean the paint. brush I was using. I decided to start a fire in the

gear locker, figuring I could make it look like it has started itself and nobody could tell the difference because it would be all burned up.

CJ I would estimate it was right around 0130 when I got back to the barracks. I didn't see anybody up and around, so I went to the MAA's Cleaning Gear Locker, took the cap 'off of the can of paint thinner, and tipped it over on to the floor. I figured it would look like it got kicked over and the cap had fallen off. I then ripped the cover off of a magazine that was in a trash can in the passageway, lit it with my lighter, and when it was burning pretty good, I threw it into the gear locker and closed the door.

I then went back outside and hid behind the trash dumpster which is on the north side of the building. I guess it was about three or four minutes later that I heard the fire alarm go off and everybody came piling out of the barracks.

Like I said, I started the fire, but I only did it to get SYKES in trouble. I did not intend that SYKES or anybody else would get hurt. I am sorry it happened, and maybe if I had not been drinking it would not have happened. During the time I was at the Melody Lounge I would estimate I drank five or six bottles of beer.

This statement, consisting of this page and 1 other page(s) was typed for me by Special Agent John R. Straightshooter as we discussed its contents. I have read and understand the above statement. I have been given the opportunity to make any changes or corrections I desire to make and have placed my initials over the changes or corrections. This statement is the truth to the best of my knowledge and belief.

Signature: _____

Sworn to and subscribed before me this _____ day of _____ in the year _____ at

_____.

Witnessed:_____ _____
Representative, Naval Criminal Investigative Service
AUTH: DERIVED FROM ARTICLE 136,
UCMJ (10 U.S.C. 936) AND 5 U.S.C. 303

Appendix 2: Military Suspect's Acknowledgement and Waiver of Rights

Place: NCISFO Mayport, FL
Date: November 1, 2001

I, Hardin, Max McTough, BT3 USN, 987-65-4321, have been advised by Special Agent Frank N. Ernet that I am suspected of the robbery of BM3 Raymond S. Mean on October 12, 2001 outside the Enlisted Men's Club Naval Station Mayport, FL in violation of UCMJ Article 122.

I have also been advised that:

1) I have the right to remain silent and make no statement at all;
(2) Any statement I make can be used against me in a trial by court martial or other judicial or administrative proceeding;
(3) I have the right to consult with a lawyer prior to any questioning. This lawyer may be a civilian lawyer retained by me at no cost to the United States, a military lawyer appointed to act as my counsel at no cost to me, or both;
(4) I have the right to have my retained lawyer and/or appointed military lawyer present during this interview; and
(5) I may terminate this interview at any time, for any reason.

I understand my rights as related to me as set forth above. With that understanding, I have decided that I do not desire to remain silent, consult with a retained or appointed lawyer, or have a lawyer present at this time. I make this decision freely and voluntarily. No threats or promises have been made to me.

Signature :_____

Date & Time: _____

Witnessed: _____

_____

STATEMENT

At this time, I, Hardin Max McTough, BT3 USN, 987-65-4321, desire to make the following volun statement. This statement is made with an understanding of my rights as set forth in the Suspect's Acknowledgement and Waiver of Rights form of November 1, 2001, 9:30 AM. It is made with no threats or promises having been extended to me.

The following is a verbatim transcript of the proceeding surrounding the taking of a statement from the undersigned, Hardin Max MCTOUGH, at Naval Criminal Investigative Service Resident Agency, Bremerton, WA on November 1, 2001. Present: Special Agent Frank N. ERNEST, LT Ernest P. DEFENDER, JAGC, USNR, Miss Ada LOTT, and MCTOUGH. The interrogation of MCTOUGH began at 0930, November 1, 2001.

S/A ERNEST: MCTOUGH, I am Special Agent Frank ERNEST, Naval Criminal Investigative Service. You have seen my credentials before, but I am showing you them again at this time for purposes of identification. This is Miss Ada LOTT. She is a NCIS Representative assigned to this office. She will record everything we say here and prepare a transcript for review by you and your lawyer, LT DEFENDER, and for your signature.

Now, before I ask you any questions, I want to advise you of your rights. You are suspected of the robbery of BM3 Raymond S. MEAN, USN, which occurred outside the EM Club on Wednesday night, October 27, 2001. You have the right to remain silent and make no statement at all. Any statement you do make may be used as evidence against you in a trial by court-martial or other judicial or administrative proceeding. You have a right to consult with a lawyer prior to any questioning. This lawyer may be a civilian lawyer retained by you at no cost to the United States, a military lawyer appointed to act as your counsel without cost to you, or both. You have the right to have such retained lawyer and/or appointed military lawyer present during this interview. And, you may terminate this interview at any time, for any reason. Do you understand your rights?

MCTOUGH: Yes I do.

ERNEST: Do you wish to remain silent?

MCTOUGH: No. I'II talk to you.

ERNEST: LT DEFENDER, your appointed military counsel is present. Do you wish to consult further with him at this time?

MCTOUGH: No ..We've already talked .

ERNEST: Let the record indicate that at 0930, November 1, 2001, that BT3 MCTOUGH acknowledged his rights in regard to self incrimination, waived his right to silence, and acknowledged the presence of his lawyer, LT Ernest P. DEFENDER. Now, for the record, please state your full name, rate, social security account number, and duty station.

Continuation of voluntary sworn statement of
Hardin Max McTough, BT3 USN, 987-65-4321
on November 1, 2001

MCTOUGH: Hardin Max MCTOUGH, BT3, USN, 987-65-4321, USS NEVERSINK

ERNEST: What is your date of birth?

MCTOUGH: January 18th, 1986.

ERNEST: What is your place of birth?

MCTOUGH: Roughhouse, Texas.

ERNEST: Before we get into any questions concerning the robbery of MEAN I would like to place you under oath. This is completely voluntary on your part. Are you willing to swear to tell the truth in your answers?

MCTOUGH: Sure. LT DEFENDER already talked to me about that.

ERNEST: Would you please stand, facing me, and raise your right hand? Do you, Hardin Max MCTOUGH, swear that the statement you are about to give is the truth, the whole truth, and nothing but the truth? So help you God?

MCTOUGH: I do.

ERNEST: What did you have to do with the robbery of MEAN?

MCTOUGH: I didn't rob MEAN. I was the one that put him down on the ground, but I did not take his wallet or money.

ERNEST: Why did you, "...put him down on the ground?"

MCTOUGH: Well, MEAN and I have had a bad thing going aboard the ship for more than six months now.

ERNEST: What do you mean, "...a bad thing going?"

MCTOUGH: There is bad blood between us. We don't like each other. We have had a few fights. Also, last month, when the ship was at Norfolk, VA I got decked from behind by somebody while I was walking on the dock, returning to the ship off liberty. I was by myself at the time, and by the time I got back on my feet after being decked, whoever hit me was gone. I reported what happened when I got back aboard the ship, but there was nothing they could do about it, other than to call Base Security. I told a Security Patrolman what happened, and that was the end of it. MEAN was not aboard the ship when I reported what happened, so I got to thinking he was probably the guy responsible. The guy who decked me. The following day I accused MEAN of doing it. He didn't deny it, he just told me to prove it. That convinced me that he was the one who ambushed me.

ERNEST: Do you recall the exact date that happened?

MCTOUGH: Well, it was a Friday night. Either the last Friday in September or the one before that.

ERNEST: What does that have to do with the robbery of MEAN?

MCTOUGH: Well, Wednesday evening, around 2200, I went to the EM Club and saw MEAN drinking there, by himself. I figured it was about time I got even with him for what had happened at Pearl Harbor. I knew which way he would probably have to go from the EM Club to the ship, so I decided to wait for him. I found a piece of board outside the building which I figured I could use. I waited for about a half an hour and MEAN finally came out of the Club. I hid between a couple of cars and waited for him to go by me. He went down like a ton of bricks.

ERNEST: What happened to his wallet?

MCTOUGH: I don't know. When he hit the ground I heard somebody yell. I cut out and made my way back to the ship. Somebody else had to take it.

ERNEST: What time would you say it was when this happened?

MCTOUGH: I guess around 2230. I wasn't looking at my watch.

ERNEST: How big was the board?

MCTOUGH: It was a one by four about four feet long. I hit him with the broad side of it.

ERNEST: What did you do with it?

MCTOUGH: I threw it down by a building, about a block away after I started running. I'm not sure I could even find it if I want to.

ERNEST: Were you running in a straight line before you dropped the board? Or did you zig zag between buildings?

MCTOUGH: I was running in a straight line at that time. ERNEST: What clothes were you wearing that night?

MCTOUGH: The same ones you guys took from me yesterday aboard the ship. The dark blue turtleneck shirt and the white trousers. ERNEST: Do you have any idea what happened to MEAN's wallet? MCTOUGH: Like I said, I cut out right away. I didn't even see his wallet. Maybe the guy who yelled at me took it or maybe somebody came up, acting like they were going to help MEAN, and took it.

ERNEST: How much money did you have that night?

Continuation of voluntary sworn statement of
Hardin Max McTough, BT3 USN, 987-65-4321
on November 1, 2001

MCTOUGH: The same $2.00 you guys found on me when you searched me yesterday.

ERNEST: Why did you decide to talk to me today?

MCTOUGH: I wanted to make it clear that I didn't rob MEAN. If I'm going to get in trouble, I want it to be for the real reason. Also, after you guys had taken my clothes and brought me down here for questioning yesterday, I figured you had me identified.

ERNEST: Have your answers to the foregoing been voluntary?

MCTOUGH: Yes.

ERNEST: Have you been threatened or promised anything in order to induce you to answer the foregoing questions?

MCTOUGH: No.

ERNEST: Do you understand the importance of the statement you have just given -that it may be used against you in a trial by court-martial?

MCTOUGH: Yes. I don't mind admitting I assaulted MEAN, but I.. didn't rob him.

ERNEST: You realize you have given the foregoing statement under oath. Have your answers been truthful?

MCTOUGH: Yes .

ERNEST: Have you anything you wish to add to your statement?

MCTOUGH: No.

This statement, consisting of this page and 4 other page(s) was typed for me by as we discussed its contents. I have read and understand the above statement. I have been given the opportunity to make any changes or corrections I desire to make and have placed my initials over the changes or corrections. This statement is the truth to the best of my knowledge and belief.

Signature: _____

Sworn to and subscribed before me this _____ day of _____ in the year _____ at

_____.

Continuation of voluntary sworn statement of
Hardin Max McTough, BT3 USN, 987-65-4321
on November 1, 2001

Witnessed:_____ _____

Representative, Naval Criminal Investigative Service
AUTH: DERIVED FROM ARTICLE 136,
UCMJ (10 U.S.C. 936) AND 5 U.S.C. 303

Pages 139 through 168 redacted for the following reasons:
- -
(b)(6), (b)(7)(C), (b)(7)(E)
(b)(7)(E)

NCIS-3, CHAPTER 7
RIGHTS WARNINGS AND SELF-INCRIMINATION
EFFECTIVE DATE: MARCH 2013

Table of Contents

7-1. Purpose**.** This chapter establishes the policy for providing the appropriate warnings prior to interviews and interrogations. Information contained in this chapter is based on the authorities cited in the text below. The provisions of this chapter apply to the Naval Criminal Investigative Service (NCIS) employees who conduct interviews and interrogations for criminal investigations.

7-2. Policy. The collection of evidence and the preparation of criminal cases are basic NCIS special agent responsibilities. Rules have been established under the laws of the United States to control the collection and introduction of evidence at criminal trials. Before a confession or admission of an accused may be admitted into evidence over defense objection, several legal considerations stemming from the Fifth and Sixth Amendments to the Constitution and Article 31(b) of the Uniform Code of Military Justice (UCMJ) must be addressed. Specifically, admissions by persons accused of a crime will be scrutinized to ensure the statements were voluntarily given under conditions that did not violate the suspect's constitutional rights. To ensure custodial interrogations do not produce statements taken against the will of the suspect, a warning must be given to suspects describing the rights afforded them under the Constitution of the United States. Additionally, a confession or admission will also require corroboration by independent evidence before it may be considered against the accused on the question of guilt or innocence. It is the responsibility of the NCIS special agent who conducts an interview or interrogation to ensure it is conducted in compliance with this chapter and applicable law.

7-3. Cancellation. NCIS-3, Chapter 7 - Rights Warnings and Self-Incrimination dated October 2007.

7-4. Chapter Sponsor. The chapter sponsor for this chapter is the Counsel to the Director, Code 00L.

7-5. Basic Concepts

a. Fifth Amendment Rights. The pertinent part of the Fifth Amendment to the United States Constitution states, "No person … shall be compelled in any criminal case to be a witness against himself." The privilege against compulsory self-incrimination has been interpreted to apply to any judicial or quasi-judicial proceeding or investigation which may furnish a lead on which a criminal prosecution may be based. An individual who is entitled to the protection of the privilege does not have to differentiate between answers, which may or may not have an incriminating tendency; rather, the individual is under no obligation to answer at all. In contrast to the Sixth Amendment right to counsel which attaches upon preferral or indictment, the Fifth Amendment affords a criminal suspect the right to remain silent any time during any questioning by law enforcement that may lead to an incriminating response.

b. Sixth Amendment Rights. The pertinent part of the Sixth Amendment states, "In all criminal prosecutions, the accused shall enjoy the right … to have the Assistance of Counsel for his defense." The Sixth Amendment attaches upon preferral of charges or indictment and prohibits law enforcement from deliberately eliciting incriminating statements from the defendant without assistance of counsel or voluntary waiver.[1]

c. Miranda Warnings. In *Miranda v. Arizona*, 384 U.S. 436 (1966), the Supreme Court ruled that statements made during a custodial interrogation by a defendant were inadmissible at a criminal proceeding unless the defendant received a full warning of his constitutional rights. Prior to *Miranda*, an individual's statement or confession was admitted into evidence if it was deemed "voluntary" based on the "totality of circumstances" surrounding the admission or confession. As a result of *Miranda*, the suspect in custody and under interrogation must be warned that he has a right to remain silent, that any statement he makes may be used as evidence against him at trial, and that he has a right to the presence of an attorney, either retained or appointed.[2]

d. Article 31(b) Warnings. Article 31(b) states, "no person subject to this chapter may interrogate, or request any statement from an accused or person suspected of an offense without first informing him of the nature of the accusation and advising him that he does not have to make any statement regarding the offense of which he is accused or suspected and that any statement made by him may be used as evidence against him in a trial by court-martial." The United States Court of Appeals for the Armed Forces held that Article 31(b) applies to agents of

[1] The right to the assistance of counsel under the Sixth Amendment is offense specific. The retained or appointed counsel of the accused is required only when the accused is being questioned about the offenses for which he or she has been charged; however, custodial interrogations concerning uncharged criminal acts remain subject to the 5th Amendment right to counsel which must be affirmatively waived. *See McNeil v. Wisconsin*, 501 U.S. 171 (1991).

[2] In addition to any required rights warnings, a confession or admission will also require corroboration by independent evidence before it may be considered against the accused on the question of guilt or innocence. Military Rules of Evidence (M.R.E.) 304(g).

military criminal investigative offices and may also apply to other civilian investigators if they are acting as an instrument of the military determined by 1) degree of control by military authorities, or 2) degree to which the civilian investigation has merged into the military investigation.[3]

7-6. Who Must Warn Suspects

a. NCIS Civilian Special Agents. Civilian special agents are required to provide Article 31(b)/*Tempia* warnings when they conduct interviews and interrogations of persons suspected of a crime who are subject to the UCMJ, pursuant to M.R.E. 305(d)(1) and *United States v. Tibbets*, 1 M.J. 1024 (C.M.A. 1974).

b. Persons Acting on Behalf of NCIS, Other Law Enforcement Agencies, or the Military. Any person acting as an agent for NCIS, other law enforcement agencies, or the military who questions a person suspected or accused of a crime must provide the required warnings to suspects (i.e., 31(b)/*Tempia*, *Miranda*, or both) prior to questioning or custodial interrogation. This may include any of the following:

(1) Other Federal Investigators. Normally, other federal investigators and non-DoD civilian police are not required to give Article 31(b)/*Tempia* warnings to military suspects when acting independently from military control. However, when the scope and character of the cooperative efforts demonstrate that the separate military and civilian investigations have merged or the civilian investigators act in furtherance of a military investigation or as an instrument of the military, the civilian investigators are required to give the Article 31(b)/*Tempia* warnings.[4]

(2) Foreign Police. If special agents or military authorities participate in, conduct, or direct interrogations of military personnel by foreign interrogators, the Article 31(b)/*Tempia* self-incrimination warnings are required. Of note, United States personnel do not participate in a foreign interrogation merely by being present, acting to mitigate damage to property or physical harm, or acting as an interpreter.[5] Information elicited from a military suspect during an interrogation by foreign police in a foreign country may be used in a court-martial only if it meets the test for voluntariness.[6]

(3) Private Citizens. In the civilian community, a private citizen has no responsibility to give warnings to other citizens when questioning that person about a suspected offense. Persons acting in a private capacity, having no connection with an official investigation, are not required to provide Article 31(b) warnings. The ultimate inquiry is whether the individual, in the line of

[3] *United States v. Payne*, 47 M.J. 37, 43 (CAAF 1997).

[4] *See id.*

[5] M.R.E. 305(h)(2)

[6] *Id.*

duty, is acting on behalf of the government or is motivated solely by personal considerations when seeking to question someone suspected of an offense. For example, a victim of a barracks larceny, attempting to recover money, has no duty to warn a suspect prior to questioning when acting for personal benefit and without official sanction; however a Master-at-Arms investigating the offense on behalf of the command would be required to warn the suspect prior to questioning.

(4) Medical Professionals. During the course of an investigation, some members of the medical profession may be questioned as witnesses regarding their knowledge of pertinent facts in a specific case. Medical personnel should not be used to elicit information from a suspect that the special agent could not obtain from the suspect without benefit of an appropriate warning. If a doctor obtains information about the suspect or patient's alleged crime that was not required for a medical diagnosis or treatment without benefit of an appropriate warning, the special agent should use a "cleansing warning" before interrogating the suspect.

c. NCIS Civilian Special Agents May Be Required to Issue Cleansing Warnings. When a suspect in a NCIS criminal investigation has made prior admissions to persons who may have been acting on behalf of law enforcement or the military, the special agent must determine the nature and circumstances during which the prior admission was made. If the circumstances required that the suspect be warned and he or she was not warned or was given defective warnings, the special agent should obtain a written acknowledgement and cleansing warning (described in the following section) prior to additional questioning or custodial interrogation.

7-7. Required Warnings

a. *Miranda* Warnings are required for custodial interrogations of persons suspected of a crime punishable under state or federal criminal law.[7] In the case of *Miranda v. Arizona*, the Supreme Court ruled that, in order to effectively secure the Fifth Amendment privilege against self-incrimination during a custodial interrogation, statements made by a suspect in such settings may not be introduced into evidence at the suspect's federal or state criminal trial unless investigating officers have effectively advised the suspect prior to interrogation of: (1) the right to remain silent and the consequences of waiving that right, particularly that the suspect's statements can and will be used against him in court; and (2) the right to consult with a lawyer and have the lawyer present during interrogation, and the right to have a lawyer appointed to represent him if the suspect is indigent.[8]

b. 31(b) Warnings are required for interrogations (custodial or non-custodial) or requests for statements from anyone suspected of a crime punishable under the UCMJ. Article 31(b) states "no person subject to this chapter may interrogate, or request any statement from an accused or

[7] Federal criminal law refers to criminal offenses codified under Title 18 of the United States Code. The jurisdictional and procedural requirements for these offenses are distinct from criminal offenses against the Uniform Code of Military Justice, which are codified under Title 10.

[8] 384 U.S. 436 (1966).

person suspected of an offense without first informing him of the nature of the accusation and advising him that he does not have to make any statement regarding the offense of which he is accused or suspected and that any statement made by him may be used as evidence against him in a trial by court-martial." Article 31(b) imposes the additional requirement that the suspect be informed of the nature of the accusation or suspected criminal conduct.[9]

c. Both *Miranda* and 31(b) Warnings are required for custodial interrogations of persons suspected of a crime punishable under state or federal criminal law and the UCMJ. *Miranda* was made applicable to military suspects who are in custody by *United States v. Tempia,* 37 C.M.R. 249 (C.M.A. 1967). In *Tempia*, the United States Court of Military Appeals held that, in addition to the required warnings of UCMJ Article 31(b), the constitutional protections of *Miranda* apply to military members during custodial interrogation.

d. Acknowledgements and cleansing warnings are required when prior warnings were lacking or insufficient. When a suspect in a NCIS criminal investigation has made admissions prior to the initiation of the investigation, the special agent must determine the nature and circumstances during which the prior admission was made. While most suspects are properly warned of their rights in the course of those investigations, occasionally suspects are not warned, are given defective warnings, or are victims of an illegal search. Those oral or written admissions or confessions may be inadmissible at any subsequent trial because of a defective warning. Prior questionable admissions or confessions obtained from a suspect must be documented and full particulars obtained relative to the previous warning provided to the suspect. If the prior interrogation involved a written statement by the suspect, the statement should be recovered and made an attachment to the Report of Investigation (ROI). The ROI should also have, as attachments, any command investigative report or documentation regarding the matter, including any waiver of rights form used. If no written documentation of the full advisement given to the suspect exists, the previous interrogator should be questioned for details of the exact warning given. When it is suspected that an existing criminal admission was improperly obtained from a suspect, the suspect must be advised that his or her previous illegal admission cannot be used against him or her in a criminal trial. See Civilian Suspect's Acknowledgement and Cleansing Waiver of Rights (NCIS Form 5580/5 (1/2001)) and Military Suspect's Acknowledgement and Cleansing Waiver of Rights (NCIS Form 5580/19 (1/2001)). If there is any doubt about whether or not to provide a cleansing warning; the better practice is to provide the cleansing warning.

[9] It is not necessary that an accused or suspect be advised of each and every possible charge under investigation, nor that the advice include the most serious or any lesser-included charges being investigated; nevertheless, the accused or suspect must be informed of the general nature of the allegation, to include the area of suspicion that focuses the person toward the circumstances surrounding the event. *United States v. Pipkin*, 58 MJ 358 (2003) (describing in dicta factors that might be considered to determine sufficiency of the warning such as, "whether the conduct is part of a continuous sequence of events, whether the conduct was within the frame of reference supplied by the warnings, or whether the interrogator had previous knowledge of the unwarned offenses . . . [and] the complexity of the offense at issue."

e. Additional Warnings and Safeguards for Custodial Interrogations of Juvenile Suspects.[10] The federal Juvenile Delinquency Act, located at Title 18, United States Code, Sections 5031 to 5042, applies to anyone under the age of eighteen suspected of committing a federal crime; however it does not apply to a member of the military accused of a crime under the UCMJ.[11] Federal courts are divided on whether the Act applies to juveniles arrested on a military installation.[12] Section 5033 requires an arresting officer to immediately advise the juvenile of his legal rights and to immediately notify the juvenile's parents that the juvenile is in custody. It also requires the arresting officer to notify the juvenile's parents of the juvenile's rights and of the nature of the alleged offense. Parental notification of the juvenile's Miranda rights must be given contemporaneously with the notification of custody.[13] If an interrogation is non-custodial, the juvenile suspect has neither a right under *Miranda* to have a lawyer present, nor a right, by statute or the Constitution, to have his or her parents present.

f. Policy Guidance Regarding the Use of Administrative Warnings. Department of Justice guidelines require that, "Under no circumstances should a prospective interviewee with foreseeable criminal exposure be interviewed under an express or implied threat that he or she will be discharged if he or she refuses to cooperate in the investigation by invoking his or her rights under the Fifth Amendment, unless this course has been discussed with and approved by the Department of Justice." The warning contained in the Civilian Employee Administrative Warning (NCIS Form 5580/4 (1/2001)) will be given when this procedure has been approved by the NCIS SSA in consultation with NCIS Code 00L and the appropriate DOJ representative. Authority to use the administrative warning must be documented by an ROI entry that identifies the person who granted the authority. Investigations wherein administrative warnings might be necessary include internal investigations controlled by the NCIS Office of Inspections (NCIS Code 00I). In those instances when assistance conducting the investigation is required by NCIS Code 00I, specific guidance will be provided to all special agents supporting the internal investigation under the cognizance of NCIS Code 00I.

7-8. Warnings Must Be Understood

a. Warnings Must Be Recited In Full. The duty to warn a military or civilian suspect cannot be discharged merely by asking the suspect if he is aware of his rights and receiving an affirmative reply. A full, complete recital of the contents of the warning is required.

---

[10] This section applies only to the questioning of juveniles pertaining to criminal activity of which they are suspected. For questioning of juveniles as victims of abuse, please see NCIS-3, Chapter 33 for guidance.

[11] *United States v Baker*, 34 C.M.R. 91 (1963); *United States v West*, 7 M.J. 570 (1979).

[12] *Compare New Jersey in the interest of D.B.S.*, 349 A.2d 105 (N.J. Sup. Ct. 1975) *with United States v. Juvenile Male*, 939 F.2d 321, (6th Cir. 1991).

[13] *See United States v. John Doe*, 170 F.3d 1162 (9th Cir. 1999).

b. Warnings Must Be Understood. Even a verbatim reading of warnings may constitute insufficient compliance with the substantive self-incrimination requirements. The presence of any factor that may have lessened the suspect's ability to understand the warning requires the government to prove that the suspect actually understood the warning.

c. Physical or Emotional Condition of Suspect. Persons who have suffered physical injury or are obviously ill, emotionally distraught, or under the influence of alcohol or drugs may not be suitable subjects for interrogation because they may not be able to provide a voluntary waiver of their rights. Prior to conducting an interview or interrogation of such persons, the interrogator should balance the physical and mental condition of the suspect with the need for an immediate interrogation.

(1) Illness During Interrogation. If a suspect becomes ill during an interrogation, it should be terminated and the suspect offered assistance in making arrangements for medical care. Unless there is an obvious need for immediate first aid, the interrogator should not furnish or administer any medication or offer medical advice to the suspect before, during, or after an interrogation.

(2) Lack of Sleep. Suspects who have been deprived of sleep for an extended period of time should not be interrogated if his or her ability to understand the rights warning might be impaired. The interrogator must exercise good judgment in determining whether the person's physical condition warrants postponement of the interrogation.

(3) Intoxication. Persons who are suspected of being under the influence of drugs (medication, alcohol, or illegal drugs) to the extent that their ability to make a voluntary waiver of rights is impaired should not normally be interrogated. When such influence is suspected, the interrogator should consider obtaining a medical opinion regarding the suspect's suitability for interrogation.

7-9. When Warnings Are Required

a. Warnings are not required in the following situations:

(1) Volunteered (Spontaneous) Statements. Volunteered statements often occur when a person walks up to a law enforcement officer, on the street or in the office, and makes an incriminating admission or confession. They may also occur when a person is in custody. Law enforcement personnel are not required to interrupt a volunteered statement in order to warn a suspect of his or her rights. As long as the person making the volunteered admission talks and the law enforcement officer does not ask questions, the statements will be admissible in a trial. Military personnel and civilians must be properly warned if they are interrogated for additional details following their spontaneous admissions.

(2) Statements Made During the Commission of an Offense. A law enforcement officer may testify to incriminating statements made by someone during the commission of a crime.

(3) Security and Public Safety Questions. A warning need not precede questions asked by law enforcement officers for their own personal security. For example, during the execution of a search warrant, a law enforcement officer may ask a security question such as, "Do you have any weapons?" During apprehension/arrest situations, an agent who knows or suspects that the person being apprehended has a weapon may ask, "where is the gun?" for the agent's safety or the safety of others who may be in a position to be injured. These kinds of questions are permitted only if asked for safety reasons and not to elicit evidence of a crime. Follow-up questions, i.e. "where did you get the gun?" are not "security" questions. Pertinent self-incrimination warnings are required prior to asking follow-up questions.[14]

(4) Collection of Non-Testimonial Evidence. Non-testimonial evidence is evidence that usually identifies the accused. Included in this category are such things as fingerprints, voiceprints, handwriting exemplars, and the results of blood, urine, sperm and saliva tests. Law enforcement officers may compel these without violating the suspect's Fifth Amendment or Article 31(b) rights against compulsory self-incrimination. However, the Fourth Amendment prohibition against unreasonable search and seizure and the due process clause of the Fifth Amendment may apply making it necessary to obtain the appropriate authorization, subpoena, or warrant. A person subject to the UCMJ who refuses to voluntarily perform these acts may be ordered by the command authority to do the following:

(a) Exhibit a tattoo, scar, or mark on the body.

(b) Try on clothing or shoes.

(c) Place feet in tracks.

(d) Submit to the collection of biometric samples such as fingerprinting, facial image photographing, palm print image collection, and iris scans, etc., as these technologies become available.

(e) Provide handwriting and voice samples.

(f) Display external body characteristics such as gold teeth.

(g) Furnish bodily fluid samples.

(5) Foreign Nationals Abroad. In a foreign country where the United States maintains military facilities, a citizen of that, or another foreign country, may commit an offense against the property of the United States or the person or property of members of the naval forces located at the facility. These suspects are not subject to the United States law and if interrogated as criminal suspects, should not be warned in accordance with United States laws. Instead, they should be warned or advised in accordance with the procedures that control such advice in the country where the base is located. A determination with respect to whether a particular case is

[14] *See New York v. Quarles*, 467 U.S. 649 (1984).

properly within NCIS investigative jurisdiction is made on a case-by-case basis with guidance from the local Staff Judge Advocate.

b. When Warnings are Required:

(1) *Miranda* Warnings are required before any custodial interrogation.

(a) Interrogation. Interrogation includes any words or actions that law enforcement officers reasonably should know are likely to elicit an incriminating response.[15]

(b) Custodial. An interrogation is custodial when it takes place during the detention of the suspect on any charges, including those outside the subject-matter of interrogation, or any other restraint on freedom of movement tantamount to formal arrest.[16] The basic inquiry is whether a reasonable person of the age of the suspect, under the circumstances, would have felt free to terminate the interrogation and leave.[17]

(2) Article 31(b) Warnings are required before questioning when the suspect is suspected of an offense and subject to the UCMJ.

(b) Suspicion of an Offense. Whether a person is a "suspect" is an objective question that requires consideration of all the facts and circumstances at the time of the interrogation to determine whether the military questioner believed or reasonably should have believed that the service member committed an offense. Courts may apply a two-prong test to determine whether an Article 31 warning is required: (1) was a questioner subject to the Code acting in an official capacity in his inquiry or only with a personal motivation; and (2) whether the person questioned perceived that the inquiry involved more than a casual conversation.[18]

(b) Persons Subject to the UCMJ. Article 2(a) of the UCMJ delineates personal jurisdiction to include: active duty service members; cadets and midshipmen; reservists on training; retired service members entitled to pay or receiving hospitalization; prisoners of war

---

[15] *See* M.R.E. 305 (b)(2) *and Rhode Island v. Innis,* 446 U.S. 291 (1980).

[16] *See Stansbury v. California,* 511 U.S. 318 (1994); *Mathis v. U.S.*, 391 U.S. 1 (1968); *and Orozco v. Texas,* 394 U.S. 324 (1969).

[17] *See J.D.B. v. North Carolina,* 131 S. Ct. 2394 (2011) (holding that the age of the suspect is a relevant factor to determine whether a reasonable person of that age would feel free to terminate the interrogation and leave).

[18] Article 31, UCMJ, warnings are not required to be given by: (1) a military doctor, psychiatric social worker, or nurse prior to asking questions of a patient for medical diagnosis or treatment; (2) an in-flight aircraft crew chief prior to questioning, for operational reasons, an irrational crewman about possible drug use; (3) military pay officials questioning a service member about a pay or allowance entitlement; or (4) a negotiator trying to end an armed standoff, provided the discussion was truly designed to end the standoff, rather than to obtain incriminating statements to be used against the suspect at trial. *See United States v. Guyton-Bhatt*, 56 MJ 484 (2002).

and persons serving a court-martial sentence; members of the Fleet Reserve or Fleet Marine Corps Reserve; members of the National Oceanic and Atmospheric Administration Public Health Service, or other agencies when assigned to and serving with the armed forces; persons serving with or accompanying an armed force in the field during a declared war or contingency operation and, subject to treaty or international law; persons serving with, accompanying, or employed the outside the United States and its territories or persons within the geographic boundary of foreign property leased, acquired, or reserved for use by the United States, and under the control of the Secretary concerned.

(3) Requirement to Advise of Rights Upon Arrest or Apprehension. No legal requirement exists that a suspect be advised of his or her *Miranda* rights immediately upon arrest or apprehension if no questioning is intended. Where an interrogator was not the arresting agent or officer, he or she must insure that the arrestee has been advised of his or her rights and determine if he or she has exercised those rights. In addition, every agent involved in the process of advising an arrestee of his or her *Miranda* rights must document the fact that the warnings were given and the specific response, if any, from the arrestee.

(4) Interrogations with Representatives of Other Agencies. In the event that a special agent conducts a joint interrogation of a military suspect with a representative of other military or civil authorities (domestic or foreign), the special agent should ensure that the suspect is advised of his or her Article 31(b)/*Tempia* rights and warnings and that the other investigator respects those rights and warnings. If this is not feasible, the special agent should not assist in the interrogation. If the representative of the other agency is an employee of the Department of Justice (DOJ), i.e., FBI, DEA, etc., the 1984 MOU between the DOJ and the DoD relating to the Investigation and Prosecution of Certain Crimes which was incorporated into DODDIR 5525.7, "Implementation of the Memorandum of Understanding Between the Department of Justice and the Department of Defense Relating to the Investigation and Prosecution of Certain Crimes," dated January 22, 1985, which was updated in 2007 as DODDIR 5525.07, "Implementation of the Memorandum of Understanding (MOU) Between the Departments of Justice (DoJ) and Defense Relating to the Investigation and Prosecution of Certain Crimes."

(5) Interrupted Interrogations. A never-ending Fifth Amendment and Article 31(b) dilemma is the determination of the need to repeat warnings at a subsequent interrogation. The general rule is that if the warnings were given properly at the first interrogation session and if the time elapsed between the first and subsequent sessions is sufficiently short as to constitute one entire continuous interrogation, separate warnings need not be given. During subsequent sessions, the suspect need only be reminded that the previously explained warning is still in effect. Suspects will be advised of their rights prior to any interview following a lapse of time, except one following a minor break, e.g., to go to lunch, to obtain a drink of water, or to use the restroom. Provided 14 days or more has elapsed between the time of the suspect's initial release from custody and the time the suspect is taken back into custody, a suspect who has requested an attorney may be re-approached and a *Miranda* or 31(b)*/Tempia* waiver will be valid.[19]

[19] *Maryland v. Shatzer*, 130 S. Ct. 1213 (2010).

(6) Self-Incrimination Warnings and Searches and Seizures. See NCIS-3, Chapter 17, "Search and Seizure," for a discussion of the relationship between self-incrimination warnings and searches and seizures.

(7) Apprehension Situations. There is no requirement to warn a suspect of self-incrimination rights while apprehending a military suspect or arresting a civilian suspect. During the period of time that elapses during the transfer of the prisoner to the place of interrogation, the apprehending/arresting agents should refrain from questioning the prisoner unless appropriate self-incrimination warnings have been given.

c. Reporting Requirements. An ROI reporting the interrogation of a suspect shall contain a positive entry showing compliance with current legal requirements. The ROI should also report details of any advice by the U.S. Attorney, or any other appropriate civilian prosecuting attorney, which requires deviation from NCIS policy. In the event a suspect submits to interrogation and no statement or results of interview are prepared, the original rights form (NCIS Forms 5580/6/4/20) will be submitted to headquarters as attachments to the ROI reporting those interviews for permanent file retention. However, if a suspect submits to an interrogation an agent should make every effort to document what the suspect said, even if it is very limited. If a suspect submits to an interrogation, and thereafter elects to remain silent or request an attorney, the agent must document this event in addition to submitting the rights form. DOJ approval for NCIS use of the administrative warning must be documented by an ROI.

7-10. Invoking Rights

a. If suspect exercises the rights to silence or an attorney, the interrogation will be immediately terminated and the special agent will follow the guidance prescribed below. An invocation of rights may take place at any time during the interrogation, even during the interrogator's recitation of the suspect's rights. After giving applicable rights warnings, special agents may interrogate a suspect who has neither invoked nor waived his or her rights. A suspect must affirmatively invoke his or her right to remain silent or seek counsel in order to halt questioning and render any subsequent statement inadmissible at trial.[20]

b. Fifth Amendment/Article 31(b) Right to Remain Silent. In advising the suspect of the right to silence, nothing may be stated by expression or implication that would create the impression that the interrogation will continue until the suspect chooses to speak or that continued silence by the suspect in the face of the accusation might be viewed negatively by the command or by a court. If the suspect states that he or she does not want to answer questions, then no questions may be asked. The interview is terminated and the interrogator is barred from asking any more questions. Any effort to maintain a rapport with the suspect is considered a violation of the right.

[20] *Berghuis v. Thompkins*, 130 S. Ct. 2250 *(2010); see also Davis v. U.S.*, 512 U.S. 452 (1994) (holding that a suspect must unambiguously request counsel in a manner that makes clear to a reasonable officer that the statement was a request for an attorney).

(1) Exercising the Right to Silence After Waiver. Even though a suspect waives his or her right to silence after receiving appropriate warnings, he or she may state that he or she does not want to answer any additional questions. When that point in the interrogation is reached, the interrogation must be terminated because the suspect has revoked his or her consent to be questioned.

(2) Search Request After the Right to Silence Has Been Invoked. Even though a suspect invokes his or her right to silence, he or she may still be asked to authorize a consent search of any property over which he or she exercises possession or ownership. One must exercise caution to ensure that no questions are asked which would result in the suspect making a statement, either an oral declaration or physical act, which is protected by Article 31(b) or the Fifth Amendment.

(3) Contact with Suspect After Invocation of the Right to Silence. Once the suspect has invoked the right to silence, questioning must cease immediately. The suspect's choice to remain silent must be scrupulously honored. The suspect may not be approached again for questioning unless: the suspect initiates contact and dialogue; a subsequent waiver is obtained[21]; or fourteen days have passed since the suspect was in custody.[22] There should be no interrogation of a suspect who is known to be represented by an attorney, except with that attorney present. The prudent course of action is to review the facts and circumstances with NCIS Counsel (NCIS Code 00L) prior to any re-interview.

c. Right to Assistance of Counsel. The right to a lawyer is not merely a right to consult with counsel prior to questioning, but also to have counsel present during any questioning if the accused so desires. Once the accused invokes the right to counsel, the interrogation must cease until counsel has been made available unless the accused initiates further communication, exchanges, or conversations with law enforcement.

(1) Interrogations in the Presence of a Lawyer. If the interrogation of a suspect is conducted in the presence of his or her retained or appointed lawyer, questions will be directed to the suspect, not to the lawyer. While it is desirable that the suspect responds to the questions, special agents cannot limit the participation of the attorney. The special agent should neither submit to cross-examination by the attorney nor divulge evidence against the suspect unless it appears advantageous to do so under the circumstances.

(2) Classified Information. If classified information is involved in an investigation, the suspect must be cautioned that he or she may not disclose classified information to any retained or appointed lawyer, unless the lawyer has the proper security clearance. The interrogation should not be conducted in the presence of the lawyer unless he or she has obtained the proper clearance. The prospective trial counsel can assist in obtaining a security clearance for the defense counsel. Additionally, the interrogator should determine if the subject is currently

[21] If suspect asserted the right to counsel, subsequent waiver must be obtained in the presence of counsel.

[22] *McNeil v. Wisconsin*, 502 U.S. 171(1991); *see also Maryland v.* Shatzer, 130 S. Ct. 1213 (2010).

cleared to discuss the classified information, as well, prior to discussing the classified information.

(3) Right to Terminate Interrogation at Any Time. A suspect may terminate the interrogation at any time for any reason. If the suspect chooses to terminate the interrogation, no additional questions should be asked.

7-11. Waiving Rights

a. Before any admission or confession may be used after a suspect has been advised of his or her rights, NCIS special agents should attempt to obtain a written waiver of rights. The accused or suspect should affirmatively acknowledge that he or she understands the rights involved, affirmatively decline the right to counsel, and affirmatively consent to making a statement. If the suspect refuses to provide a written waiver but also does not unambiguously assert his or her right to remain silent or have the assistance of counsel, special agents must be prepared to demonstrate that a suspect has not previously attempted to exercise the right to counsel, has not affirmatively asserted the right to remain silent, and any statement of the suspect was the result of a waiver implied from the conduct or statements of the suspect.

b. Obtaining Waiver

(1) Immediately after the advisement of rights, the following questions should be asked to determine if the suspect understands and desires to waive those rights:

(a) Do you understand your rights?

(b) Do you want a lawyer?

(c) Understanding your rights, are you willing to talk to me at this time?

(2) If the suspect acknowledges an understanding of the rights, does not desire to consult with an attorney, and is willing to make a statement, the execution of the appropriate waiver form (NCIS Form 5580/20 or 5580/6) is appropriate. Although the signing of the form does not conclusively demonstrate an effective waiver, the completed form is evidence of a waiver. The individual administering the rights is encouraged to refer to the waiver form when providing the oral warning to insure that a full advisement of rights is given to the suspect and that the advisement is substantially in accordance with the language set forth on the form. The non-use of NCIS forms does not render involuntary any confessions or admissions thereafter obtained, provided the advice administered is substantially in conformance with the prescribed form and a knowing, voluntary, and intelligent waiver thereof is obtained.

c. Refusal to Sign Waiver Form – Special Warning Required. If the suspect refuses to sign the appropriate waiver form, the interrogating special agent must insure that the suspect is not expressing a desire to invoke his or her rights. Special agents should note the exact words, reasons, or refusal to sign the waiver in the interrogation log and must give the following specific

warning: "Your failure to sign the waiver does not mean that your statements cannot be used against you."

d. Waiver After Previous Invocation of Rights. If a suspect invokes one or more of the rights prior to or during an interrogation and then later elects to waive those rights and submit to interrogation, the pertinent preprinted NCIS Form 5580/20 or NCIS Form 5580/6 should be used. The circumstances surrounding the initial exercise of the rights and reasons for submitting to re-interrogation must be documented in a written statement taken from the suspect, results of interview prepared, or in the ROI reporting the interview.

7-12. Voluntariness

a. To be admissible as evidence against an accused, a pre-trial statement taken from a suspect during interrogation must have been made after a knowing, voluntary, and intelligent waiver of rights. An express waiver of a suspect's rights may be ineffective if it is established that it was not in fact "knowingly, intelligently, and voluntarily" made.

b. Voluntary. For a statement to be admissible at trial, it must be made voluntarily subsequent to a voluntary waiver of rights. The statement will be deemed involuntary if obtained by use of a threat, promise, inducement, duress, or physical or mental abuse amounting to coercion or unlawful influence. Whether a statement was made voluntarily and rights were waived voluntarily is not based on the belief of the investigator but rather on the totality of the circumstances. The following factors may be considered under the totality of the circumstances analysis by the courts when determining voluntariness:

(1) Physical Violence or Threats. No qualification may be placed on the right to remain silent. Consequently, an issue of "voluntariness" is raised if the suspect is told that continued silence will lead to more severe charges, consequences, or punishments.

(2) Confinement. The imposition or threat of confinement because of a suspect's failure to make a statement raises the issue of involuntariness.

(3) Deprivation of Comforts and Necessities. Depriving an accused or suspect of comforts and necessities may result in a deprivation of the mental freedom to speak or to remain silent. Deprivations, which may prove fatal, include the lack of sleep, medical aid, or the ordinary necessities of life.

(4) Use of Trickery, Stratagem, or Fraud. Courts may consider a waiver of rights obtained by deception as involuntary. However, once a suspect makes a valid waiver of rights, military and civilian court decisions do not generally preclude the use of deception to obtain confessions so long as the deception was not used to obtain an untrue confession. An example of the use of deception to obtain confessions is stating that an eyewitness has identified the accused, an accomplice has confessed, or the evidence is enough to close the case when the exact opposite is true. Very few court decisions hold that even intentional misrepresentation by interrogators of

the accused's factual situation makes a resulting confession involuntary. See NCIS-3 regarding general interrogation techniques.

(5) Inducements. An interrogator's statements that he or she will inform the court and prosecutor of the suspect's cooperation does not by itself render the statement involuntary; however, offering other inducements that provide a direct benefit to the suspect may render a confession inadmissible. Special agents do not have the authority to broker deals, make promises, or suggestions of leniency by the prosecutor or court. Such representations will make a statement inadmissible.

(6) Promise of Benefit to Relative(s). It is generally impermissible during the interrogation process for the interrogator to play upon the suspect's emotions. An issue of involuntariness is raised if the interrogator promises a benefit to the suspect's relative(s) to induce a confession. For example, if the special agent informs the subject that if he or she cooperates, it will not be necessary to arrest and bring in his or her spouse for questioning, any subsequent confession may be inadmissible.

(7) Adjurations to Tell the Truth. Admonishing a person to tell the truth is not coercion, unlawful inducement, or improper influence and will not invalidate a subsequent statement. However, suggestions or promises that the suspect will fare better in court if he or she confesses have resulted in the statement being held inadmissible

(8) Immunity. Justice is sometimes served by granting immunity to prospective witnesses who might otherwise invoke the privilege against self incrimination. Grants of immunity are generally controlled by statute. One who implicates him or herself relying upon an ineffective promise of immunity can bar any such statement from admission in evidence. A promise of immunity may take the form of a promise to cease the investigation and close the case, a simple promise of a confidential exchange, non-prosecution, or talk of administrative discharge. Actual negotiations, including conditions and the extent of the grant or promise of immunity, should be worked out and formalized between the individual, the Convening Authority, their respective attorneys and the court, as described below. R.C.M. 704 and M.R.E. 301(c)(1) provide the framework for immunity at courts-martial.

(a) There are two types of immunity: testimonial (or use) immunity and transactional immunity. When a witness is granted testimonial immunity, the government may not subsequently use his/her testimony, or evidence derived from it, in a prosecution against him/her. A testimonial grant is not, however, a bar to prosecution based upon independent evidence. Transactional immunity is broader. A witness who testifies under a transactional grant of immunity may not be prosecuted for any transaction, i.e., act or offense about which he/she testifies, even if the government obtains independent evidence of his/her criminal involvement. Traditionally, grants of immunity in the military have been testimonial.

(b) A prospective military witness may not reject a grant of immunity. Failure to testify after a grant of immunity has been made is punishable as a violation of Article 92, UCMJ.

JAGMAN sections 0138 and 0139 provide additional guidance regarding requests for immunity for both military and civilian witnesses.

(c) NCIS personnel must ensure that they do not cause a prospective witness to believe that NCIS can grant or directly obtain a grant of immunity. If a prospective witness solicits information about a grant of immunity, he/she should be informed that his/her interest will be made known to the proper military or civilian authority. The matter should then be referred to the Staff Judge Advocate, the Trial Counsel, or the appropriate U.S. Attorney.

(d) In unusual circumstances, subject to prior approval of the parent NCISFO, it may be appropriate for the investigating special agent or NCISRA to recommend to military commanders or appropriate U.S. Attorney that a grant of immunity be extended to a particular prospective military or civilian witness. For example, this procedure might be appropriate in a case where the testimony of one principal may be needed to convict the other principals in an offense.

(e) When a grant or promise of immunity has been approved, an interview should be coordinated with the individual's attorney, if any. The terms and limitations of immunity should be reviewed before the interview begins; the limits of the grant should also be set forth in any written statement obtained. If an interviewee provides incriminating information regarding offenses not specifically enumerated in the grant of immunity and the special agent wants to follow up with questions regarding those admissions or confessions, the special agent should provide appropriate rights advisement covering the new offense before any questions are asked.

(9) Effect of a Previous Involuntary Statement. Even if the suspect was not exposed to any additional coercive influences between the first, inadmissible statement and the second statement, the second statement may still be determined to be inadmissible because it was tainted by the coercive influence of the first statement. See section 7-7, subsection d, for guidance on issuing cleansing warnings. For the second statement to be admissible, the government must affirmatively establish that the second statement is not a product of the original coercive factors. Several factors help cleanse the second statement from the taint caused by the initial coercive factors:

(a) Elapsed time between the statements.

(b) Second statement was made to a different interrogator.

(c) Adequate warning preceding the second statement.

(d) Minimal references to the first statement at the second interrogation.[23]

(10) Physical and Mental Traits of the Suspect. To evaluate whether the will of the suspect was overborne by actions of law enforcement, courts will consider whether mental traits,

[23] *See United States v. Gardinier*, 65 M.J. 60 (2008).

physical traits, education, and age of the suspect could make the suspect more susceptible to manipulation or intimidation.

7-13. Use of Registered Sources and Undercover Agents

a. Interrogations or Questioning by Private Persons. Law enforcement cannot avert the warning requirement by employing an undercover agent or registered source to do something that they could not do themselves.[24]

b. Miranda Rights and Use of Non-Law Enforcement Cooperating Witnesses, Agents, or Proxies. The *Miranda* requirement that suspects be warned against compulsory self-incrimination only attaches in a custodial setting. Therefore, the use of a cooperating witness or undercover agent to elicit incriminating statements in a non-custodial setting does not violate these rights because the suspect is not being questioned in a custodial setting. If a suspect has previously invoked the right to assistance of counsel, a voluntary waiver must be obtained in the presence of counsel before any attempt is made to elicit incriminating statements unless fourteen days have passed since the suspect has been in custody or questioned by law enforcement or the suspect initiates further discussion. The prudent course of action is to review the facts and circumstances with NCIS Counsel (NCIS Code 00L) prior to any re-interview. See section 7-11 for additional guidance when a suspect submits to interrogation after previously invoking his or her rights.

c. Article 31(b) and Use of Non-Law Enforcement Cooperating Witnesses, Agents, or Proxies. Where a questioner is performing a law enforcement or disciplinary investigation, and the person questioned is subject to the UCMJ and suspected of an offense, then Article 31 warnings are required; whether the questioner should be considered to be performing such an investigation is determined by assessing all the facts and circumstances at the time of the interview to determine whether the military questioner was acting or could reasonably be considered to be acting in an official law-enforcement or disciplinary capacity.[25] Undercover agents or sources acting at the direction of NCIS special agents are considered to be acting on behalf of law enforcement.

d. Sixth Amendment Right to a Lawyer. The Sixth Amendment attaches upon referral of charges or indictment. When law enforcement officers plant even passive listeners, those who do not stimulate conversation about the crime charged, around the accused after referral of charges or indictment this violates the Sixth Amendment right to counsel.[26] The Sixth Amendment is also offense specific, meaning counsel retained for charged offenses does not necessarily need to be present for questioning the suspect about uncharged criminal conduct; however such questioning may violate the Fifth Amendment right to counsel. Anytime a suspect

[24] For more information on this topic see Section 7-6 *supra*.

[25] *United States v. Cohen*, 63 M.J. 45 (2007).

[26] *United States v. Henry*, 447 U.S. 264 (1980).

is represented by an attorney, and questioning the suspect regarding uncharged criminal conduct outside the presence of counsel is contemplated, NCIS Code 00L should be consulted.

7-14. Disclaimer. The NCIS 3 Manual, including this Chapter, is set forth solely for the purpose of internal agency guidance. The Manual is not intended to, does not, and may not be relied upon to create any rights, substantive or procedural, enforceable at law by any party in any matter, civil or criminal, and it does not place any limitations on otherwise lawful activities of the agency.

Page 187 redacted for the following reason:
- - - - - - - - - - - - - - - - - - - -
(b)(7)(E)

CHAPTER 9
TITLE: CRIMINAL REDUCTION OPERATIONS
POC: CODE 23B
DATE: SEP 08

APPENDICES:

9-1. GENERAL

The establishment of a NCIS-wide proactive effort to identify and interdict criminal activity has been recognized as being essential to the successful accomplishment of its investigative mission. The NCIS criminal operations effort will be accomplished through either Special Operations (SO) or Undercover Operations (UO). This chapter addresses policy and procedures to be followed in establishing and maintaining criminal operations.

9-2. DEFINITION AND PURPOSE

9-2.1. General. A criminal operation is any organized effort, originated by a NCIS component, to surface and interdict criminal activity affecting the Department of the Navy (DON). This includes, but is not limited to, the utilization (b)(7)(E) (b)(7)(E)

9-2.2. Criminal Operation. The primary purpose of a criminal operation is to provide the NCIS with a proactive as well as reactive capability in dealing with criminal depredations within the naval service. Each operation will be based on previously developed credible intelligence that criminal activity does in fact exist, and at such a scale to justify the concentrated application of sophisticated investigative techniques. Once an operation identifies individuals involved in the targeted criminal activity, appropriate investigations will be initiated to compile evidence, which will result in meaningful judicial or administrative action. Additionally, proliferation of operations should be avoided. (b)(7)(E)

(b)(7)(E)

9-2.3. Initiative Operations. Initiative operations are reserved for significant problems, and the objective of these operations will be specific and realistically attainable. As such, inquiries to determine the existence of a problem will be completed prior to consideration to conduct an operation. (b)(7)(E)

(b)(7)(E)

9-3. CRIMINAL OPERATIONS DEVELOPMENT

9-3.1. A basic step in developing a criminal operation is the identification of suspected high crime or problem areas within a command, unit or area. An operation will normally have more potential for success if specific problem areas rather than entire commands are targeted. Methods of identifying such depend largely upon local conditions and the initiative of the special agents (SAs) involved; however, the following are some methods where potential operational target areas have been identified areas in the past:

a. Routine complaints from commands that a problem exists or is believed to exist, but specific criminal activity and suspects are unknown.

b. (b)(7)(E)

c. Results of fraud and crime surveys.

d. Analysis of known or reported losses of property by a command to include volume of material surveyed as lost or misplaced during a given period.

e. Reports of inspection or review, which indicates that security conditions within a command, provide an opportunity for criminal activity to flourish.

f. Indications that deficiencies revealed during previous crime surveys, audits, Inspector General reports, etc., have not been corrected after a reasonable period of time.

g. Unexplained frequent cash overages or shortages in units responsible for appropriated or non-appropriated funds.

h. Frequent inventory shortages, which are treated routinely by command personnel as being "paperwork errors."

i. Frequent irregularities in stock records or in cash flow records.

j. A series of unsolved crimes such as burglaries, rapes, assaults, etc., in a specific geographical area.

9-3.2. Once the existence of criminal activity has been established and a specific target area has been defined, a tentative operational plan should be formulated to include operational objectives and a proposed method of approach to the problem. See Section 9-13 for special consideration in developing operations in such areas as conspiracy, Racketeer Influenced and Corrupt Organization (RICO) violations and "reverse stings". Planning should include the type and number of assets needed, i.e., SA support required, amount of funds necessary to support the operation, and possible assistance needed from the command, federal and local law enforcement agencies. The command will be notified before further positive action is taken. To prevent compromise and therefore necessitate the need to abort the operation, command personnel must exercise care to limit knowledge of operations. Once the initial planning is completed, the ROI (OPEN) should be submitted NCISHQ (See Section 9-4).

9-3.3. (b)(7)(E)

(b)(7)(E)

9-3.4. (b)(7)(E)

(b)(7)(E)

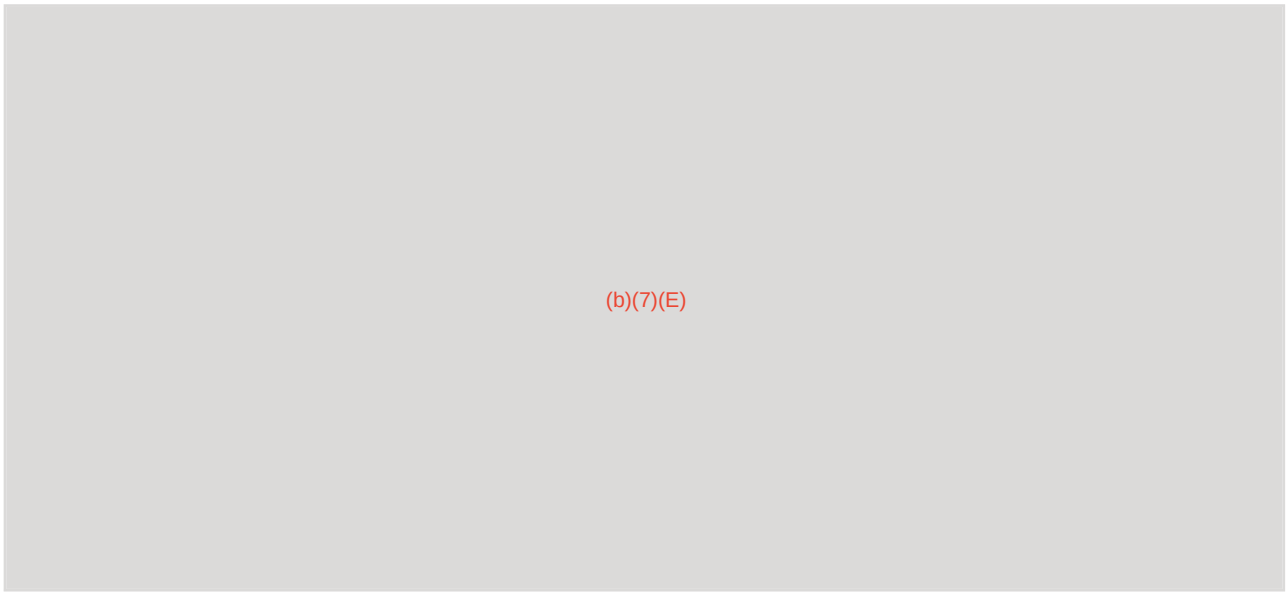
(b)(7)(E)

9-3.5. (b)(7)(E)

(b)(7)(E)

9-3.6. All Group II operations are approved, funded, and monitored at the NCIS Field Office (NCISFO) level and Special Agent In Charge (SAC) concurrence for the operation will be set forth in the opening document.

9-3.7. Criteria For Group I Operations. When an operation in any investigative category requires, by NCIS or a cooperating agency, one or more of the following, it becomes a Group I operation:



9-3.9. The productive phase of any criminal operation involves the initiation of criminal investigations to document evidence gleaned against suspects within the target area. Appropriate investigation(s) will be initiated and all evidence subsequently obtained via the operation and other investigative efforts will be documented in the Report of Investigation (ROI). A criminal operation may result in many criminal investigations of various categories before it is completed. Termination of an operation should occur only after evidence of criminal activity has abated and the operation has met its objectives.

9-3.10. All initiative operations should be specific in scope with a well-defined goal. Group II operations will require revalidation by NCIS Code 23 after the first 90 days and every 90 days thereafter. This will be accomplished by an action/lead to NCISHQ (Code 23B) in sufficient time to allow for a response before revalidation date. The ROI (ACTION) to NCIS Code 23B will document SAC concurrence for continuation of the operation. The documentation will set forth the operational direction in sufficient detail to allow for evaluation of the need to continue the operation and the likelihood of success in obtaining its objectives. If revalidation is disapproved, the operation will be closed by the control NCISRA.

9-3.11**.** As a matter of policy, NCIS will not initiate operations (UO/SO) targeting homosexuals and related consenting adult sex crimes.

9-4. CRIMINAL OPERATION REPORTING PROCEDURES

9-4.1. The initiation, status and termination of a criminal operation will be reported through the standard NCIS investigative reporting system. NCIS-1, Chapter 25, provides standard report writing policy; however this paragraph provides specific report writing policy that pertains to criminal operations reporting. Header and title information for criminal operations reporting will

be prepared in conformance with NCIS-1, Chapter 25. (b)(7)(E)

(b)(7)(E)

9-4.2. Criminal Operation (Open)

(b)(7)(E)

Pages 194 through 196 redacted for the following reasons:
- -
(b)(7)(E)

(b)(7)(E)

9-4.7. Aside from the standard 30-day reporting requirement, a ROI should be submitted whenever the basic operational plan has changed or when significant events occur during the operation. An example would be when the operation is about to change from a covert phase to overt and press releases/conferences are planned. The 30-day reporting period will begin from the date of the most recent ROI submission.

9-4.8. Reporting Results Of The Operation. The medium for reporting detailed results of the criminal activity developed from the operation will be the NA/MA investigations initiated; these reports will be provided to the cognizant command or prosecutor. Keeping operational security in mind, the command will be kept apprised of the status of the overall operation. (b)(7)(E)

(b)(7)(E)

General information developed during the course of an operation and not reported in a specific initiated investigation should be reported in a ROI(INFO) (collection report) and provided to command if appropriate. This information would include such things as administrative anomalies, security weaknesses and any other information, which should be brought to the attention of the command for possible corrections or improvements. When a Group I operation is terminated, NCISHQ will conduct a debriefing to obtain valuable information (lessons learned) for use in future pre-operational briefings.

(b)(7)(E)

(b)(7)(E) Being administrative in nature it should only be utilized for leads going to and from NCISHQ. The operation ROI should not be utilized to forward leads from office to office. As a deviation to NCIS-1, Chapter 25 for ROI (INTERIM) an “Executive Summary” is not required in an operational ROI.

9-4.9. Terminating A Criminal Operation. Once the objectives of a particular operation have been accomplished or it is determined the original suspicions within the target area are unfounded or the operational scenario is not feasible, the operation will be terminated. It is not

necessary that all NA/MA investigations generated by the operation be closed. The closing document on the operation will be an ROI that will reference, at a minimum, those investigations generated by the operation, reflecting this in the text in order to distinguish them from any other references.

a. This closing ROI will also include the final reporting period and cumulative totals of:

(1) Cases initiated and the number of suspects investigated and/or arrested; distinguished by military service, DoD civilians, Non-DoD civilians and Foreign Nationals;

(2) List of Level IV Sources utilized by number and distinguished by military service, DoD civilian, non-DoD civilian and Foreign Nationals;

(3) Number and identity of cooperating agencies;

(4) Funds expended by cooperating agencies on NCIS-related cases;

(5) Emergency Extraordinary Expense Fund (.123B) funds expended;

(6) Oral/wire intercepts conducted;

(7) Type, quantity and value of contraband or seized property, distinguished by recovery, purchase, and/or successfully seized via forfeiture proceedings; and

(8) Number of agents, by agency, utilized in a deep UC capacity and approximate number of hours spent in a deep cover role.

b. Additionally, if the operation was non-productive, a summary statement should be made regarding the probable reason for its non-productivity. If oral/wire interception was authorized but not used, a statement as to the reason for not using the technique will be included. An example of a closing operation ROI is Appendix (6). Should significant operational information develop during an NA/MA investigation after the operation was closed, a supplemental ROI should be submitted.

9-4.10. The disposition code for all closed criminal operations will be /C.

9-5. NCIS CRIMINAL OPERATIONS RECORD SYSTEM

Criminal operation documentation will be maintained in the various elements of NCIS in the same manner and for the same periods of time as other investigations. NCISHQ will maintain the file as a "generic case", i.e., 5-year retention. Group II operations will be maintained for 5-year retention and Group I operations will be maintained for 15-year retention.

9-6. (b)(7)(E)

CHAPTER 10
TITLE: DOCUMENT EVIDENCE AND IDENTIFICATION
POC: Code 24B3
DATE: JUL 08

10-1. GENERAL

10-1.1. Forensic Document Evidence normally consists of a piece of paper bearing handwritten entries in ink or pencil, typewriting, or other machine-generated text. The term “document” may also be applied to any surface bearing writing, marks or symbols applied by varied media, such as spray-paint writing on a wall, scratched or carved letters on a door or plane canopy, etc.

10-1.2. Each document tells a story, transmits a message, or in some manner depicts the thoughts or intention of the author. Most Department of Defense document investigations involve forged or altered medical prescriptions, anonymous letters, forged or worthless checks, and various types of military, government, and non-government forms.

10-2. FORENSIC DOCUMENT EXAMINATIONS

10-2.1. Forensic Document Examinations generally attempt to identify or eliminate suspect writers (or machines) as the source of questioned features on a document. When results of these examinations are presented in court, sometimes through a Forensic Document Examiner's expert opinion testimony, they are often sufficient to complete the case against a suspect.

10-2.2. Some questioned documents require that several types of Forensic Document Examinations be performed. In addition to the identification of handwriting, Forensic Document Examinations include typewriting, alterations, erasures, date determination, photocopy machines and copies, computer printers, fax machines, multi-function office machines, charred and water-soaked documents, indentations, inks, paper, rubber stamps, shredded-paper document reconstruction, and various others.

10-2.3. Forensic Document Examinations seek to reveal the pertinent information present in each item of evidence. Whether the examination results in an elimination or identification of a writer or machine as the source of a questioned document, or provides other information concerning a document, depends upon the features observed in the evidence. Background information from an investigation does not influence the examination results. The objectivity of Forensic Document Examinations has been demonstrated by the fact that approximately 40% of USACIL Forensic Document examinations result in no identifications being reported. The poor identifiability of respective questioned materials (i.e., bad copies) and/or inadequacies of known materials submitted for comparison (i.e., known writings not comparable with questioned writings) are most frequently the source of limited findings in Forensic Document Examinations. The accuracy of handwriting identification and other Forensic Document Examinations results, are constantly reviewed via proficiency testing performed by all USACIL examiners.

10-3. THE IMPORTANCE OF HANDWRITING

10-3.1. Handwriting is still prevalent in many business transactions and personal matters. Handwriting imparts the desired personal touch that individualizes documents and, in many cases, makes them legally acceptable.

10-3.2. There are few individual acts more identifiable than a person's handwriting. Most persons learn to write at a young age by repeating letter forms in a particular system. Writers deviate to varying degrees from the system used to teach them, with handwriting habits becoming relatively stabilized during the teenage years. An individual's visual perceptions, artistic preferences, physical nervous system control, muscular coordination, and other factors, collectively influence the development of each writer's handwriting habits. The handwriting habits of adults tend to be as firmly fixed as any other personal habit.

10-3.3. Each writer's handwriting habits are unique. Though writers may share varying numbers of similarities in their handwriting features with other writers, no two writers have ever been found whose handwriting habits were indistinguishable. When provided with identifiable questioned writing and sufficient known writings for a comparison examination, a properly trained Forensic Document Examiner can accurately identify the writer of questioned writings, and conversely, eliminate those who did not make a questioned writing.

10-4. HANDWRITING IDENTIFICATION

10-4.1. Handwriting identification examinations generally involve the comparison of questioned and known writings to determine the author of the questioned writing. Examinations may also involve comparing questioned writings with other questioned writings to determine whether they were written by the same person. A forensic handwriting examination involves assessing the similarities and differences of the features among two or more sets of writings. The Forensic Document Examiner's (FDE) assessment of the quantity and quality of the accumulative similarities and differences, forms the basis of the Examiner's opinion.

10-4.2. Handwritten documents fall into two categories: Questioned and Known

a. Questioned Writings - These writings generally involve some doubt as to their authenticity.

b. Known Writings – These writings are recognized as being genuine, proven, or acknowledged writings by a writer. The two types of known writings are: Standards and Exemplars.

c. Standards refer to known writings executed outside the scope of (and normally prior to) an investigation. Standards are also called "Non-requested Writings", "Unsolicited Writings", "Course-of-Business Writings", or "Pre-existing Writings". Standard writings are those that are known to have been authored by an individual in the normal course of personal or business writings. Examples of standards include signatures on service record documents, cancelled checks from an individual's personal checking account, personal letters, etc. During a handwriting examination, standards provide a demonstration of a person's normal handwriting habits. Standards are usually written before an investigation, but when there is too great a time differential between the standards and questioned writing, the value of the standards may be reduced. For example, the writing of a young schoolboy may differ in many essentials from his mature writings made later in life.

d. Exemplars refer to known writings made by a writer (suspect, victim or witness) at the request, and in the presence of, an investigator. Exemplars are also called "Collected Writings", "Solicited Writings", and "Prepared Writings". Exemplars repeating the questioned document entries are necessary to insure that sufficient known letterforms, letterform combinations, and other handwriting features are present to provide for a meaningful comparison between the questioned and known writings.

10-5. STANDARD KNOWN WRITINGS

10-5.1. For a productive handwriting examination to be possible, an investigator must acquire sufficient samples of a suspect or victim's known writing. Acquiring standard known writings first allows the investigator to use them as a point of comparison when Exemplars are being written later. To be of value for comparison, standard known writings should repeat as much of the questioned writings as possible:

a. Standard writings should repeat the questioned handwritten (or cursive) and hand printed letter forms.

b. Standard writings should repeat the questioned upper-case and lower-case letter forms.

c. Standard writings should repeat the slow, neatly-written letterforms, or rapid and abbreviated letter forms, etc., present in the questioned material.

10-5.2. The authenticity of standard known writings must be proven to the satisfaction of the court. Any document or writing attributed as a known writing by a specified person for a comparison examination, must be logically linked to the person who wrote them. Document origins can be established in ways that include:

a. Acknowledgement by the person who wrote them.

b. By the testimony of a witness who saw the writing being made.

c. By having an employee (often someone designated as the “record custodian”) testify about the production, handling and maintenance of the known writing document(s) during the course of daily business.

d. By the testimony of a family member, friend or other witness who is familiar with the writing of the person to whom the known writing is attributed. (Though this type of confirmation is legally acceptable in many jurisdictions, practical experience has demonstrated that this method can be very unreliable).

10-5.3. The best standards for comparison are those from the same general class as the questioned writing. For example, if the questioned signature is on a check, known writings of the suspect on other checks should be included when available. Additional sources of standard writings include:

a. The wallet or purse in the person’s possession. Identification cards, driver's license, credit cards, bankcards, etc., provide good sources of handwriting standards. Notes, shopping lists, telephone listings, etc., can also be found. Good quality copies of these personal items may be submitted if it is not possible to submit the original documents. However, original documents are always preferable.

b. Handwritten statements in the files of the local military police. Suspect writers have often been involved as witnesses or suspects in unrelated matters wherein the military police have obtained handwritten statements.

c. Education centers often have entries on file documents pertaining to service members. If the service member is participating in classes through the center, educators may have handwritten homework papers, essays or exams available.

d. Unit personnel files may contain entries on forms, test papers bearing handwritten answers (sometimes in essay form), counseling statements, handwritten letters and notes from the service member to his/her chain of command concerning disciplinary actions, appeals to unfavorable efficiency reports, requests for off-post housing, explanations of bad debts and bounced checks, and a variety of other items.

e. The service member’s workplace may contain a variety of handwriting specimens, particularly those of an office worker. You may find draft letters and reports, calendar entries, appointment books, pocket notebooks, etc. A non-office worker may make entries in clothing records, on receipts for tools and equipment, equipment logbooks, maintenance records, etc.

f. The service member’s quarters may contain unmailed letters, notes, schoolwork, financial records, canceled checks, receipts, calendar entries, personal planning notes and records, and copies of such documents as credit applications, bank account applications, and job applications.

g. Friends and relatives of the service member may possess handwritten letters, notes, greeting cards, and other correspondence by the service member.

h. Other records that may yield valuable handwriting standards include:

(1) Locator cards in unit and post mailrooms

(2) Paid finance vouchers

(3) Medical and dental records in local facilities

(4) Post vehicle registration documents

(5) Local bank and credit union records

(6) SJA claims forms

(7) SJA legal assistance records

(8) Records of the local office of the Inspector General

(9) Records of local civilian police agencies

(10) Post Exchange high value item sales forms

(11) Military club card applications

(12) Military and civilian drivers license applications

(13) Military housing records

(14) Records of the transportation office

(15) Forms in possession of local businesses, such as:

(16) Housing rental documents

(17) Real estate records

(18) Equipment rental documents

(19) Credit applications

(20) Applications for utilities services

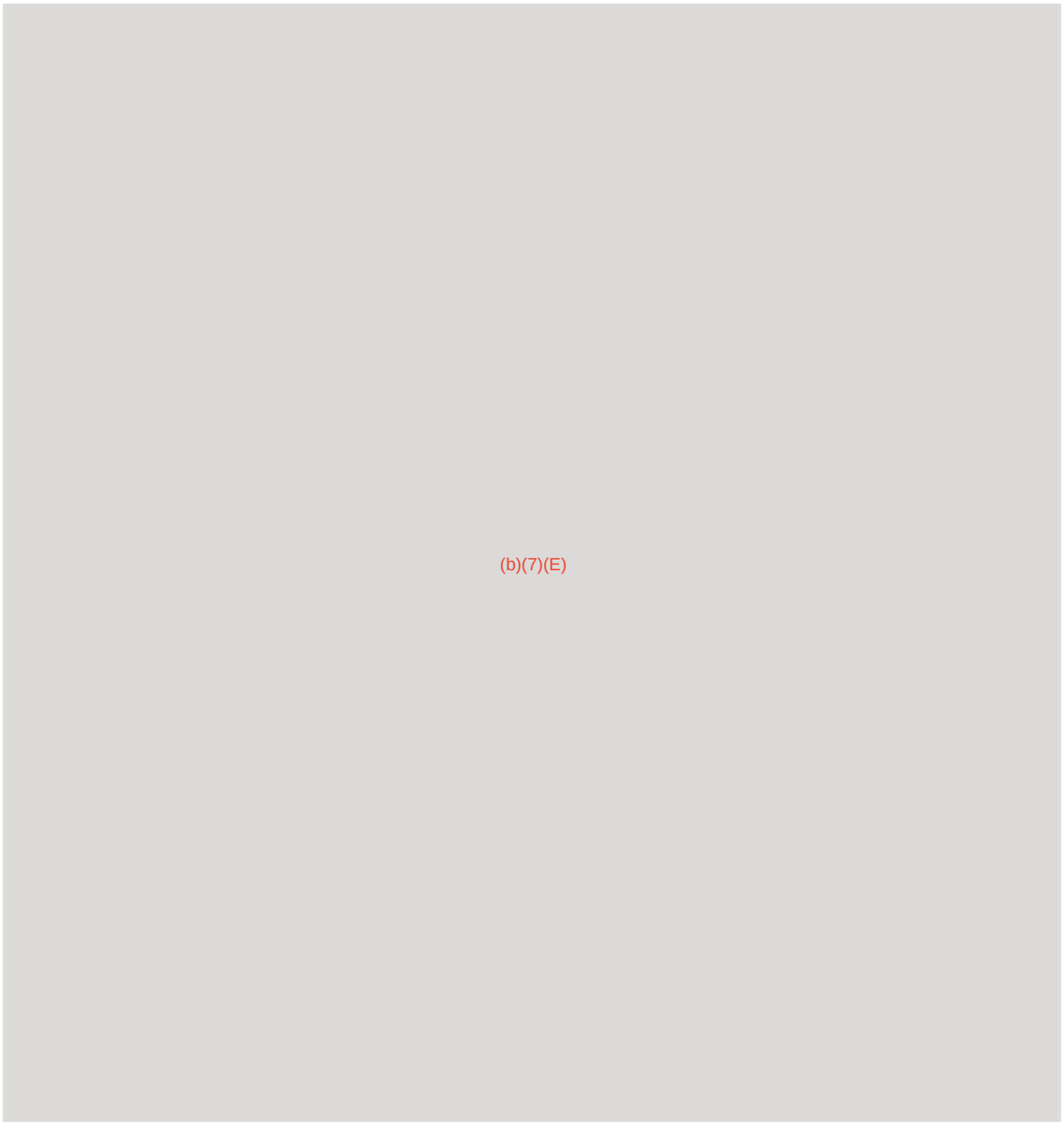
(21) Weapons purchase and registration forms

(22) Job applications

(23) Automobile purchase contracts

(24) Insurance applications

10-6. EXEMPLAR KNOWN WRITINGS



Pages 314 through 320 redacted for the following reasons:
- -
(b)(7)(E)

(b)(7)(E)

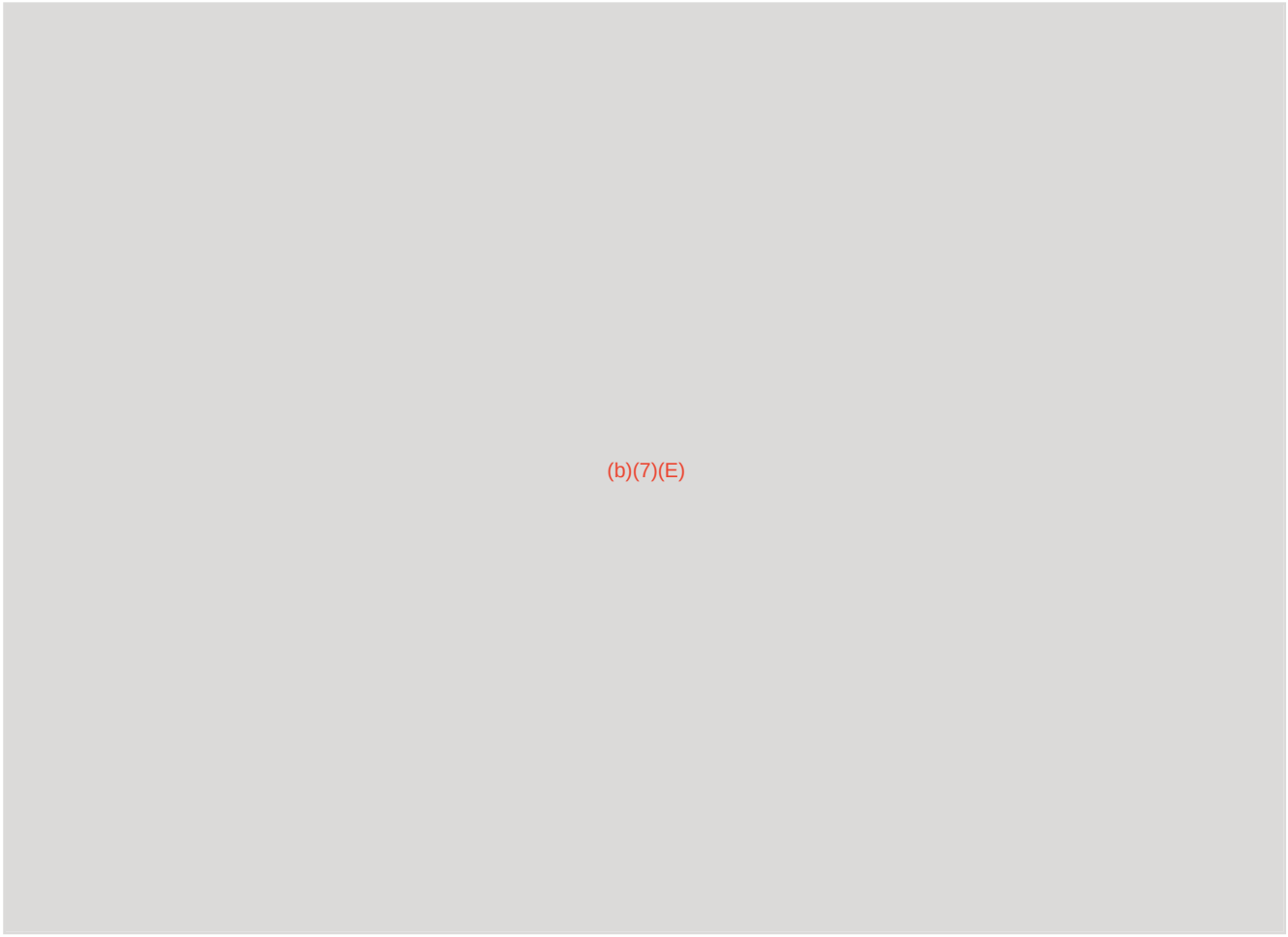
10-11. RIGHTS ADVISEMENT WARNINGS

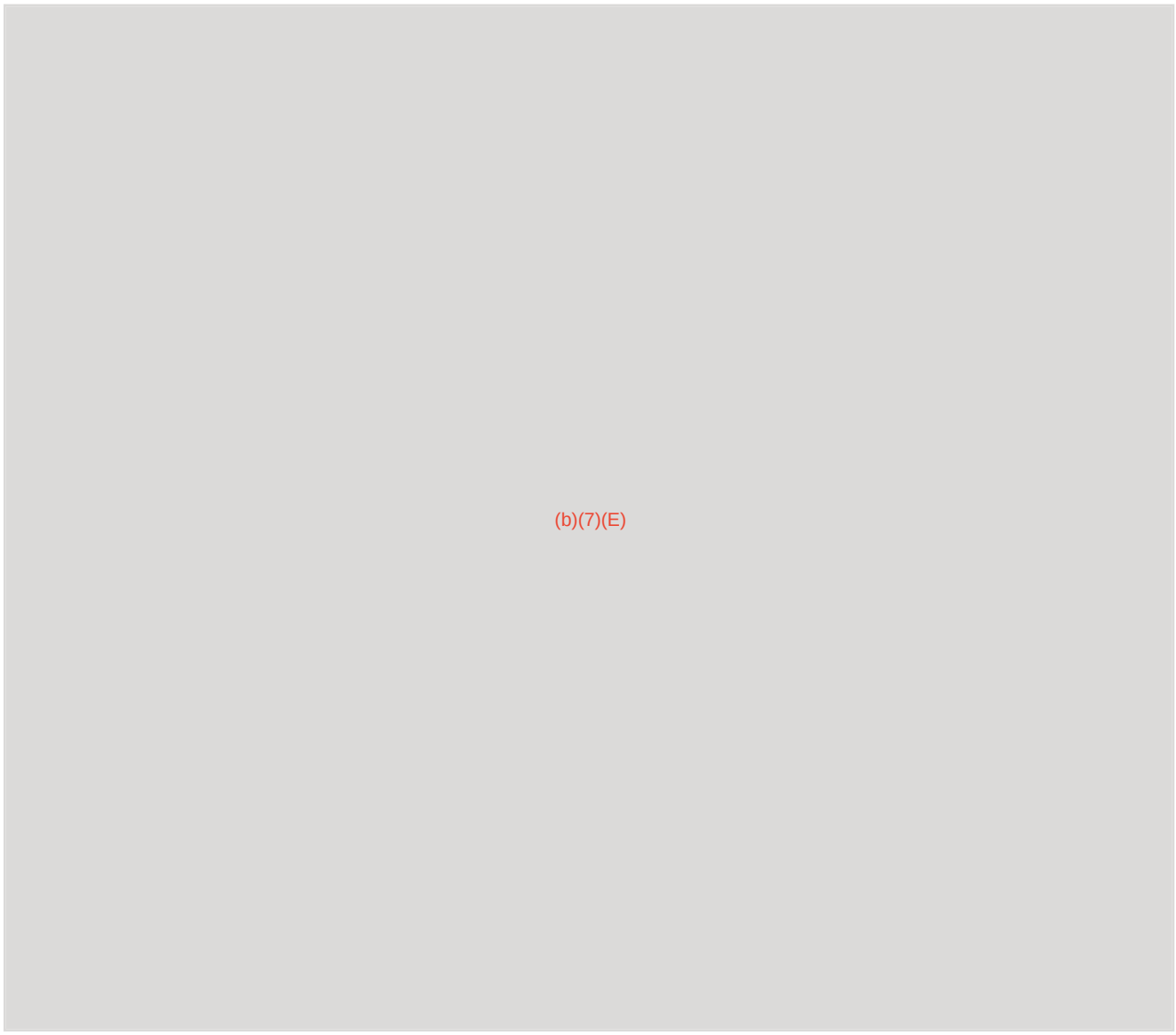
10-11.1. No self-incrimination warnings are required when requesting exemplars from military or civilian subjects, victims and witnesses. Military members can be ordered to provide

exemplars (see United States vs Airman Basic Timothy P. HARDEN, 14 M.J. 598, USAF CMR, August 13, 1982) and civilians can be compelled to provide sample writing by a court or grand jury.

10-12. ON-SITE ASSISTANCE

10-12.1. The Forensic Document Branch at USACIL has deployed examiners for several on-site assistance missions in the past. These missions allowed examiners to screen large quantities of questioned documents enabling them to extract representative samples that they judged to be most productive for future examination at the laboratory. Examiners also will screen large numbers of known writings by large suspect populations (cursory handwriting screenings of personnel forms have identified writers of hate letters, forged documents, suicide letters, etc.), resulting in rapid solutions to many investigations that involved higher command interest. These on-site screenings saved investigators from collecting unnecessarily large quantities of questioned documents and known writings, documenting them on evidence vouchers, and packaging and shipping the unnecessarily large quantities of evidence to USACIL for examination. This screening also resulted in significant time savings for USACIL that would have been involved with inventorying, marking and examining larger quantities of unscreened evidence.





Questions concerning these findings should directed to the Forensic Document Branch at DSN:

(b)(6), (b)(7)(C)

CHAPTER 11
TITLE: TECHNICAL ASPECTS OF INVESTIGATION
POC: CODE 24
DATE: MAY 08

11-1. GENERAL

11-1.1. Policy considerations concerning the use of technical investigative aids often depend on whether the investigation is purely criminal in nature or involves intelligence aspects. Executive Order 12333 promulgates procedures that apply when employing investigative aids such as electronic surveillance and closed circuit television (CCTV) in counterintelligence investigations and when such use affects United States persons. NCIS-3 Chapter 36, "Electronic Interceptions and Electronic Investigative Aids", provides additional detail concerning intercepts for criminal or intelligence purposes and annual inventory requirements. Guidance issued separately should be reviewed prior to requesting or employing those aids for intelligence purposes. The Operational Support Directorate (OSD), NCIS Code 24, consists of numerous departments and divisions, several of which provide technical investigative support other than crime scene investigation. OSD Divisions include the Technical Services Division, NCIS Code 24B1 and its detachments, the Technical Surveillance Countermeasures Support Division, NCIS Code 24B5, and the Cyber Support Department, NCIS Code 24D.

11-1.2. Often direct communication, either by telephone or in person, with OSD, can provide the most valuable assistance to the special agent. Based on the nature of the request, a secure means of communications may be required. The investigator should describe in detail the specific situation faced, and depending upon the situation encountered, may receive techniques or guidance. Usually, the best advice can be provided before requiring an action. Early contact with the appropriate OSD element is suggested, particularly in the case of special operations and wide-ranging cases needing funds or specialized equipment.

11-1.3. While the supporting technical departments and divisions can often provide guidance on analysis of the resultant data, the actual analysis is a case agent's responsibility. Making regular periodic downloads help prevent modern equipment from rapidly overwhelming and outstripping analytical capabilities.

11-2 TELEPHONES, WIRELESS DEVICES, AND COMPUTERS

A substantial body of law exists concerning what can and cannot be done involving telephones, wireless devices, and computers. Consult the NCIS Headquarters (NCISHQ) Legal Office, NCIS Code 00L, prior to attempting interception of telephones, wireless device, or computer communications. NCIS Codes 24B1 and 24D have devices for this purpose.

11-3. VOICE IDENTIFICATION AND AUDIO ENHANCEMENT

Although NCISHQ no longer maintains an in-house capability for voice identification, NCIS Code 24B1, and its regional detachments can assist field special agents in obtaining quality audio recordings which can then be submitted to the Federal Bureau of Investigation laboratory for voice identification analysis. NCIS Code 24B1 and detachments have the capability to perform limited enhancement on audio recordings. Enhancement is not a substitute for a quality recording and cannot replace what is not already there.

11-4. CLOSED CIRCUIT TELEVISION (CCTV)

11-4.1. CCTV evidence has brought many NCIS investigations to a successful conclusion. Cases particularly suited to CCTV surveillance are those in which the action or events which constitute the crime under investigation, predicted with reasonable degree of certainty, will (1) occur at a specific fixed location, and (2) be observable by the hidden video camera. Typical examples include theft of money or property from cash registers, lockers, security cages, and freight loading docks and cases of malicious destruction targeting specific objects or areas with the likelihood of being targeted again. Video surveillance is not useful in resolving cases in which the investigation has not progressed to the point of establishing a probable and a specific, definable location at which the crime is being perpetrated. Typical examples of no-hope video surveillances are those cases involving inventory losses at warehouses, commissaries, or exchanges where determination of an actual crime is uncertain. Special agents should remember that CCTV cameras cannot look around, seek out, and zero in on criminal activity; they can only monitor a single location at which activity is likely to occur.

11-4.2. Some practical considerations to keep in mind when considering video surveillance:

a. Lighting. Illumination levels slightly below that of the average office normally are sufficient. Lower levels, however, may downgrade video quality to the point of being unusable. Depending on the site requirements, some illumination may be added. Limited quantities of specialized illumination devices are available.

b. Concealment. Inspect the target for possible camera concealment modalities, particularly taking note of false ceilings; they afford ready-made camera concealment and facilitate installation in a number of other ways as well. Utilize desks, cabinets, lockers, and other containers if securable and the risk of discovery can be sufficiently minimized. A limited number of mobile or portable platforms are available.

c. Installation. Installation and concealment of a video camera and transmission link may

take as long as ten minutes or in excess of ten hours depending on the type of installation needed and conditions encountered. Undetected access to the target area by the installation team and the reasonable assurance of privacy during the installation process are absolutely essential.

d. Listening Post (LP). Another important consideration of video surveillance is to secure space in which to locate the video monitor and recorder at the receiving end of the video link. Examples of good LPs are lockable unoccupied Bachelor Officers Quarter rooms or offices, closets, utility rooms, and telephone closets which are within range of the particular video transmission used (hard-wire, wireless, or microwave) and accessible to the special agent as often as may be necessary without arousing suspicion in the target area. Experience has shown that attempts to merely hide the LP equipment in an active office area, for example, the exchange officer's office in a Navy Exchange installation, usually results in compromise. LP security is a must and should consider operational security needs. The fewer persons involved and the fewer intrusions into the area of concern, the more likely of successful technical support.

11-4.3. Laws regarding the use of CCTV are neither as restrictive nor as clear as those regarding wiretaps or audio eavesdropping. Careful thought should be given to the type of area considered for a CCTV installation. Places such as offices, cashier booths, and strong-room doors pose no problem, but residences or rest rooms can be difficult. Operators should consult NCIS Code 00L, prior to attempting installation of CCTV or other clandestine surveillance technology in these types of spaces.

11-5. OPTICAL SURVEILLANCE

This technique includes methods to assist in providing visual observation of activities which would not normally be accessible by the investigator because of such limiting factors as distance, low light level conditions, obstructions, etc. This includes the use of cameras, closed circuit television systems, binoculars, infrared viewers, and night vision devices. The use of such equipment does not require NCISHQ approval but must comply with existing federal laws and privacy regulations.

11-6. ELECTRONIC SURVEILLANCE

Included in this category are such additional techniques as electronic alarm devices, motion and body heat detectors, agent signaling, and vehicle tracking devices. Limited numbers of each are available through NCIS Code 24B1 and its subordinate detachments. Oral/wire intercept of audio and collateral information is discussed in more detail in NCIS-3 Chapter 36, “Electronic Interceptions and Electronic Investigative Aids”. While not all such equipment requires the Director's approval for use, legal and privacy aspects must be considered in the use of such techniques. Questions concerning the NCIS policy or legality of such techniques should be resolved, by NCISHQ if necessary, prior to their use.

11-7. TECHNICAL CONSUMABLES

In addition to technical investigative assistance available from NCIS Code 24B1 and its detachments, a great variety of consumable supplies and kits are obtainable through the Security

and Logistics Department, NCIS Code 11A. While many of the supporting technical entities will provide an initial or starter issue of consumables, the user is responsible for obtaining and maintaining adequate working materials. An inventory of supplies and material available from NCISHQ is issued periodically.

11-8. NON-TRADITIONAL INVESTIGATIVE TECHNIQUES

11-8.1. Overview. Non-traditional investigative techniques are unique or exceptional investigative methods employed during the course of an investigation or inquiry. These techniques are infrequently utilized and are not required during most investigations. A ruse video is one example of a non-traditional investigative technique. Many of these techniques may require assets not normally possessed at the field office and may require substantial lead and preparation times. Early contact with the appropriate supporting entity is suggested.

11-8.2. Definitions. Video/documentation ruse technique is the use of videotape or other media and information (i.e., audio, documents, photographs, artifacts) for the purpose of creating an environment which leads the suspect or target to believe investigators are in possession of data that corroborates allegations of suspected criminal and/or illegal activities of the subject.

11-8.3. Approval Procedures. Case agents considering the utilization of the above techniques will fully document the reasons for use in consultation with the appropriate experts (i.e., legal, prosecutor(s), technical), to ensure that equipment is utilized in compliance with United States and Host Nation laws and regulations. Prior to utilizing a non-traditional investigative technique in an investigation, the case agent must gain Special Agent in Charge or Deputy Assistant Director approval. The approval process and implementation of a non-traditional investigative technique will be thoroughly documented in the case file as well as in the Report of Investigation. When considering the use of non-traditional investigative techniques, case agents and field supervisors are encouraged to coordinate with appropriate NCISHQ codes to obtain assistance in the development of investigative strategies and establishing courses of action. When employing non-traditional investigative techniques, NCIS will comply with existing policies and procedures.

11-9. SUMMARY

The special agent is encouraged to maintain an awareness of new materials and techniques within the field of police science and consider the use of technical investigative aids if appropriate.

CHAPTER 12
TITLE: PHYSICAL EVIDENCE AND THE CRIME SCENE
POC: Code 23A
DATE: DEC 07

12-1. GENERAL

12.1.1. In connection with criminal investigations, physical evidence may be defined as articles or material found in an investigation which will assist in the solution of the crime and the prosecution of the criminal. Physical evidence is often much more valuable to an investigation than testimonial evidence. Physical evidence does not lie or equivocate; it can only be misinterpreted. Thus, translators are required to tell a jury what the evidence is saying. It is the purpose of this chapter to familiarize investigators with the language of evidence so that such misunderstandings do not occur.

12-1.2. Such evidence obtained during the investigation of a criminal case may be of great value in assisting the investigator in solving the crime by reconstructing the crime and assist in identifying the criminal. By using physical evidence found at the scene of a crime or the personal nature of the evidence found, such as fingerprints, clothing with special marks or other such articles, it is possible to reconstruct the manner in which the crime was committed or identify the individual who committed the crime. The physical evidence may also be used to validate or refute an alibi.

12-1.3. In addition to being of such tremendous value in solving the crime, any evidence that is obtained is likewise of great assistance in the prosecution of the criminal in court by demonstrating complicity. Physical evidence tends to speak for itself. It simply needs a translator to tell the jury what it is saying. The "translator" must thoroughly understand the "language" of evidence, or risk giving incorrect information. Without such physical evidence directly linking a suspect to a crime, successful prosecution would be difficult, if not impossible.

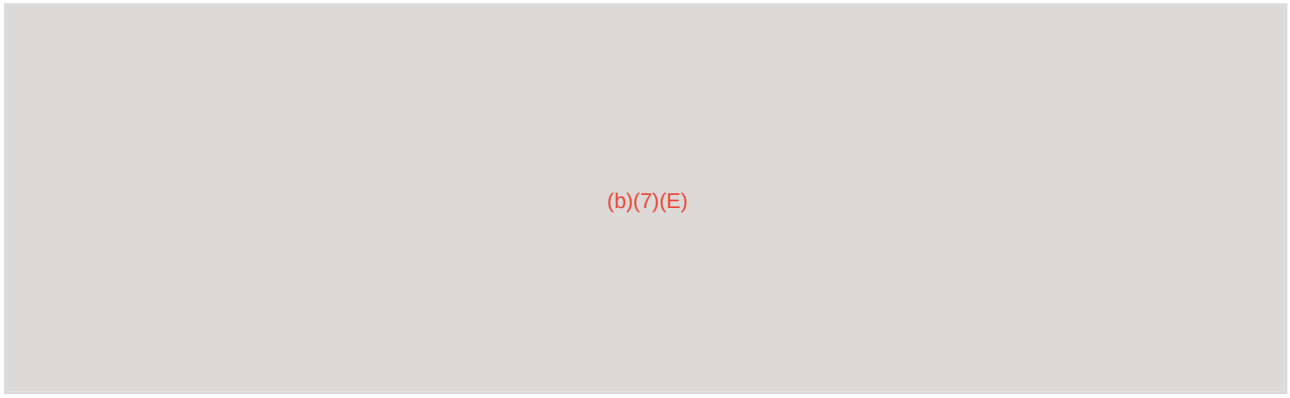
12-1.4. In considering evidence found at the scene of a crime, the investigator is confronted with two distinct types of evidence: fixed or immovable evidence, such as footwear impressions in the soil, tire prints in mud or on paved highways, latent fingerprints on immovable objects or on objects which are too bulky to remove readily; and movable or removable evidence which can be discovered at the scene of the crime, properly preserved and identified and later used either to assist in the solution of the crime or the prosecution of the criminal in court.

12-1.5. The ultimate value of physical evidence is determined by how useful it is throughout the investigation and into trial. It must retain its value from when the evidence was first found, until the conclusion of all judicial proceedings. Investigators must be aware of this requirement and take appropriate measures to ensure that any piece of evidence will retain the maximum evidentiary value. This chapter discusses appropriate methodology for searching and sketching a crime scene, collecting, handling, preserving, examining and marking various commonly encountered types of physical evidence for identification. Evidence concerning fingerprints, documents and casts and molds will not be specifically addressed in this chapter.

12-2. COLLECTION AND PRESERVATION OF PHYSICAL EVIDENCE-BASIC CONSIDERATIONS

12-2.1. The scene of any crime is itself evidence, and the testimony of a trained investigator concerning observations and findings at an unchanged crime scene is vitally important to the successful resolution of the case. Improper protection of the crime scene will usually result in the contamination, loss, or unnecessary movement of physical evidence items, any one of which is likely to render the evidence useless. Therefore, the first investigator to arrive at the scene of the crime automatically incurs the serious and critical responsibility of securing the crime scene from unauthorized intrusions. Even though the individual who arrives first might have searched it for physical evidence, the necessity to immediately take precautions to protect it remains unchanged.

12-2.2. Obviously, there is no definite rule or set of rules that can be applied to defining the dimensions of the scene of a crime. (b)(7)(E)



12-2.3. Obviously, in order to professionally and successfully process the scene of a crime for the presence and recovery of physical evidence, the crime scene searcher must be properly equipped. All NCISRAs should ensure their equipment holdings include an adequate number of fully stocked and readily available crime scene kits. Ideally, these Crime Scene Search Kits should be stored in vehicles assigned to the NCISRA and should be routinely inspected so that depleted supplies may be restocked. Crime scene supplies should be obtained from the Major Case Response Team (MCRT) crime scene supply coordinator (see section 12.21 of this chapter).

12-2.4. The discovery and collection of physical evidence through meticulous and professional crime scene search methods and procedures can be irreparably negated through improper packaging of collected evidence. Following the collection of evidence, extreme care must be taken to insure against loss of valuable physical evidence. Loss of physical evidence is generally experienced through improper preservation procedures and sometimes from improper packaging and shipping procedures. Guidelines for appropriate storage and shipping containers will be specifically addressed in various sections of this chapter.

12-3. SEARCHING THE CRIME SCENE

12-3.1. The success of an investigation that involves a definable crime scene depends heavily on the initial observations and actions of the first investigator to arrive at the scene. This statement is generally applicable, regardless of the type of crime. While the circumstances of each particular case will naturally govern the actions taken to protect and preserve the physical evidence, the following are considered to be generally valid guides:

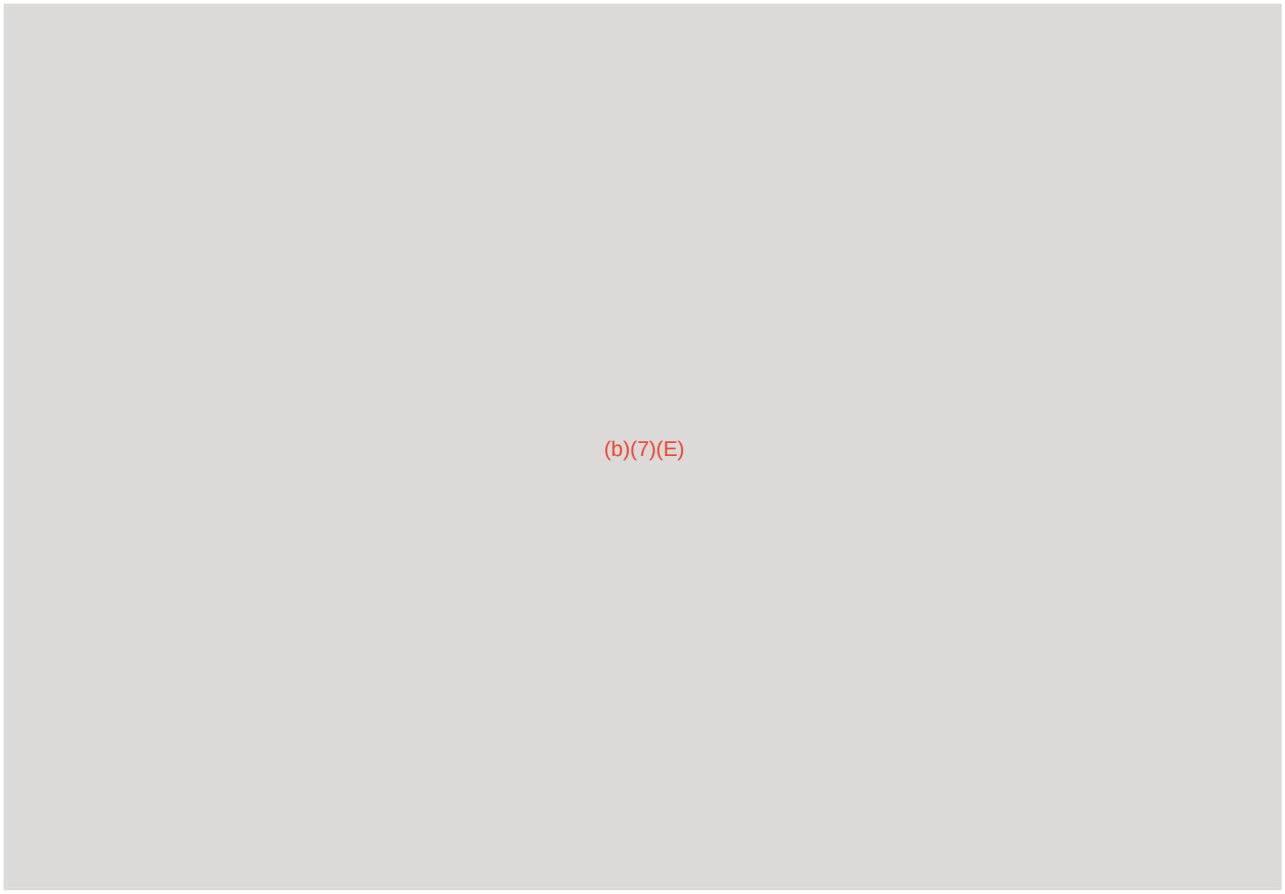
a. If injured persons or individuals who are in immediate danger are discovered at the scene of the crime, giving them aid is a matter of first priority.

b. If sufficient personnel are available, the immediate measures necessary to protect the crime scene should proceed simultaneously with giving aid to injured persons, or examining apparent deceased persons.

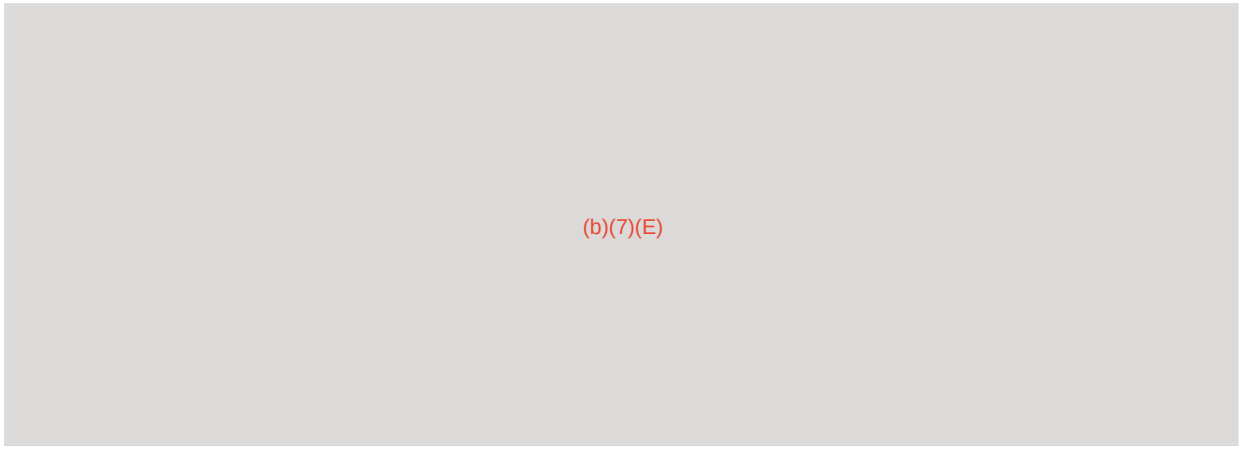
c. The immediate protective actions include roping off certain critical exits or apertures, posting guards to control spectators and souvenir hunters who may be gathering around, especially in areas expected to have high potential for physical evidence yield. Also, ensure that

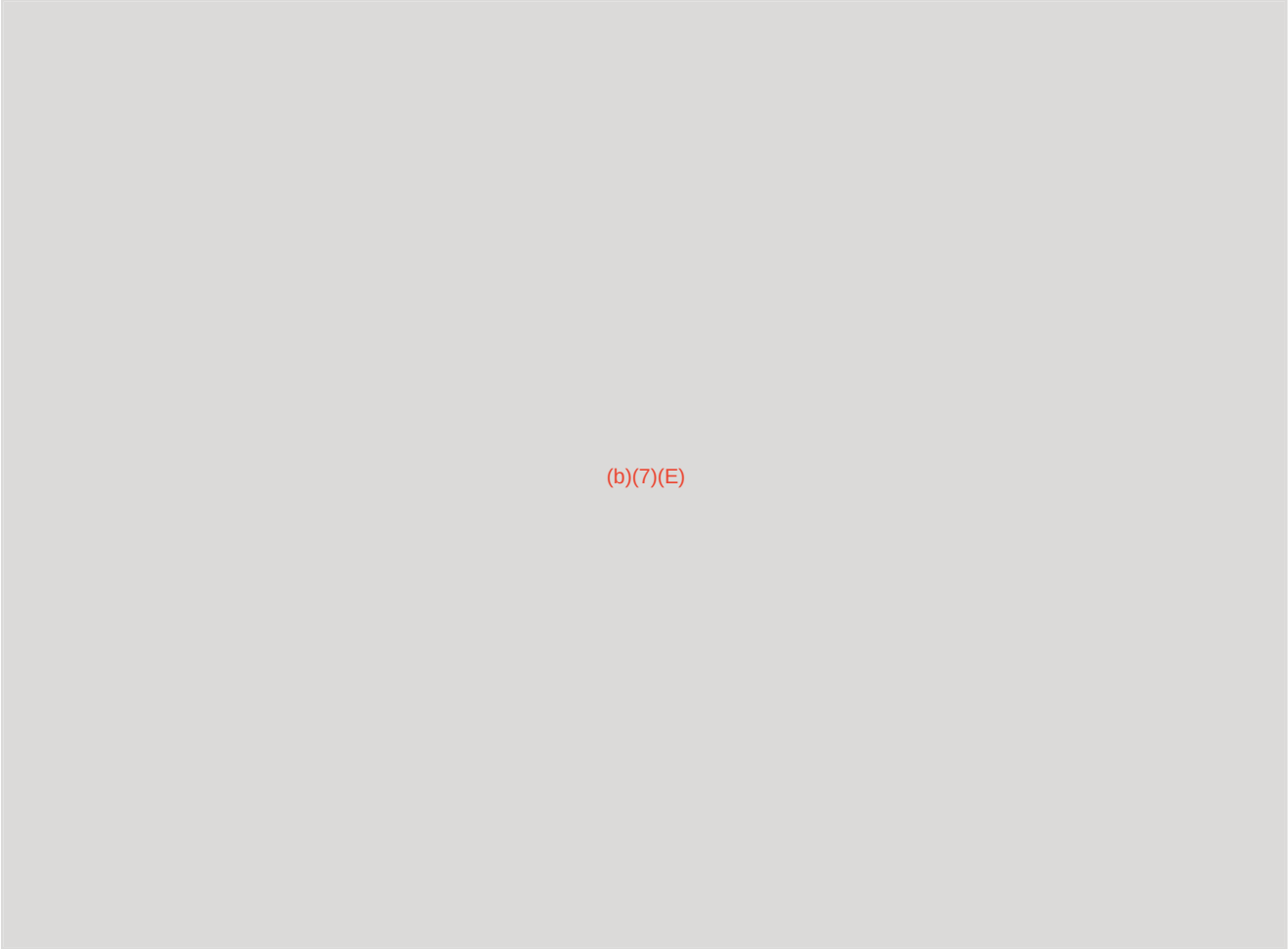
areas that would be affected by smoke, rain, snow, direct sunrays, or other environmental elements that could potentially alter any evidence are immediately covered.

d. The underlying intent of all actions taken to protect the scene of a crime is to preserve physical evidence so that the investigating agents or laboratory examiners may review it in detail. The most important consideration of the individual preserving the scene is to prevent the following actions:



12-3.2. In instances where the crime or crime scene location is reported to the NCIS agent telephonically, the following procedures must be taken immediately:



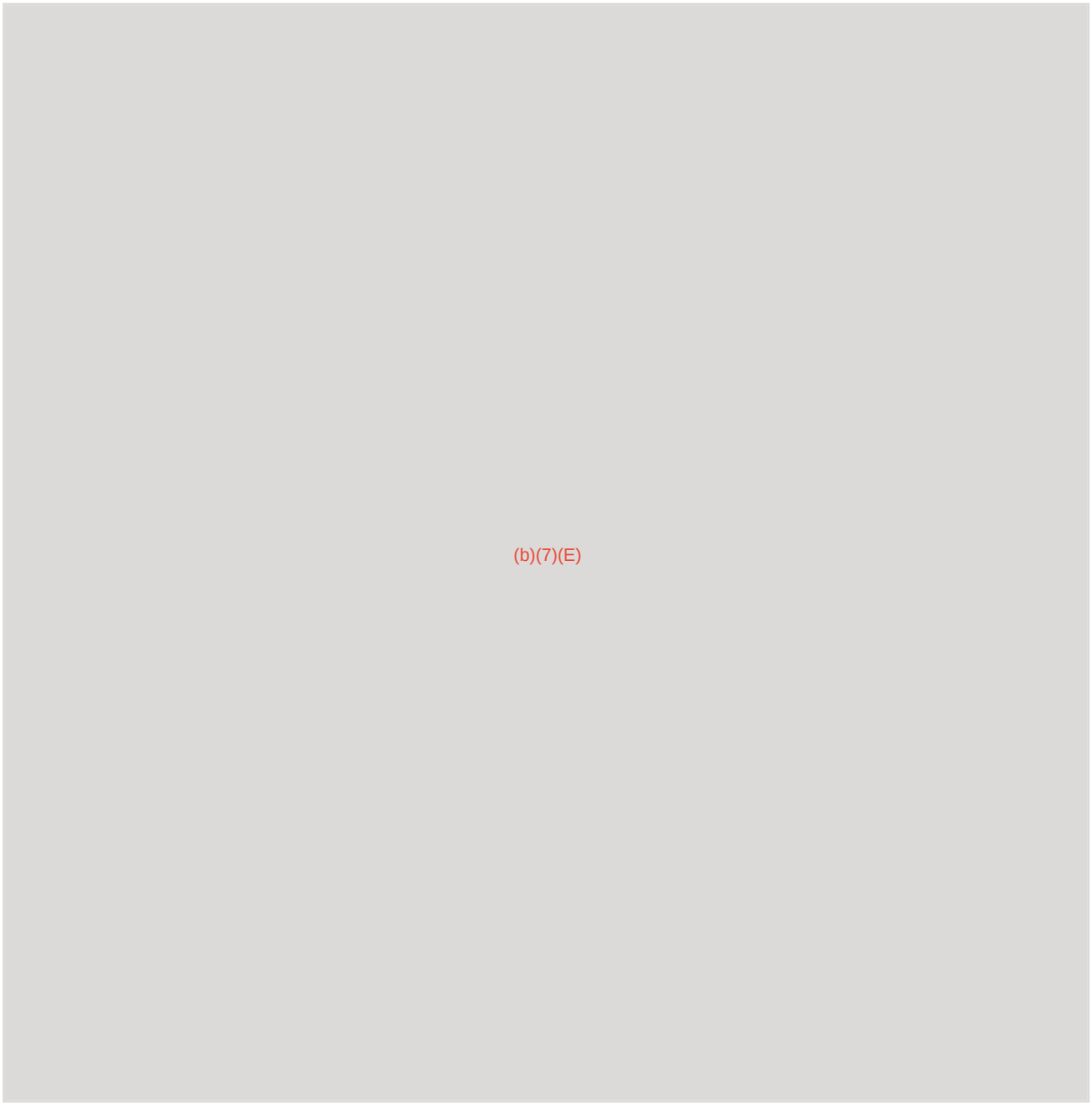


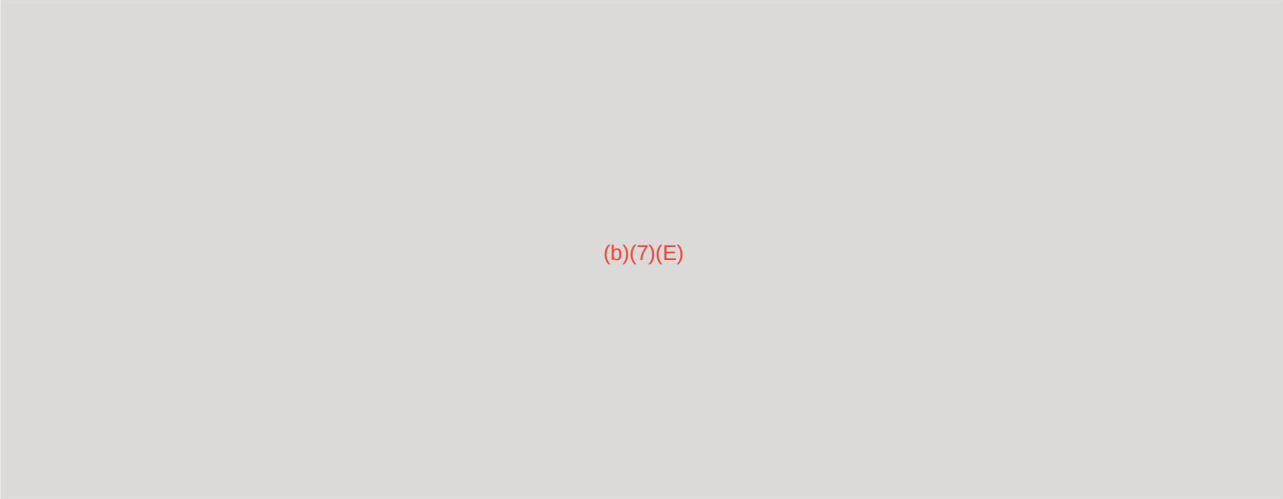
12-4. CRIME SCENE PHOTOGRAPHY

12-4.1. There are many important elements of crime scene photography that should be recognized. The discipline of crime scene photography is very dynamic and requires adaptation depending on the location, crime, victim and many other variables. Photographers should follow guidelines that are extremely important to the proper documentation of a scene. The ultimate goal of an investigator is to capture the scene as accurately as possible and as it is found. Each piece of evidence must be photographed before it is collected as evidence. Everything of evidentiary value must be documented. It is for this reason that the photographer and sketcher need to work closely together and what each does must augment the other. Documentation of each photograph is often times just as important as the photograph itself. The investigator needs to keep a log that details important information for each picture that is taken. Information that needs to be noted in a log includes, but not limited to, a description of the camera, the lens, accessories, ISO (speed), photograph number and scene or view depicted. For more advanced photography and for scenes that require advance photography equipment it is recommended that the Forensic Consultant, who is trained in advanced level photography, be called upon to assist. If a video of the scene is taken before detailed scene photography is begun, the video will be treated the same as photographs attached to an IA. The video is not to be entered into the evidence custody system. (see NCIS-3, Chapter 30, Death Investigations).

12-4.2. When taking scene photos the first frame should be a photo identifier or photo card with basic information such as case number, date, location of scene and your name. As photographs are started the back of the photo card is used to record the lens used, f-stop, shutter speed and view depicted. Every photo should be logged on the photo card immediately after taking it so the camera variables are recorded before they are forgotten. The card is important because it allows past mistakes to be corrected. If one photo isn't successful, knowing the settings used and how the picture was taken may suggest an alternate way to take a similar picture in the future.

12-4.3. The three steps of coverage that are important while photographing evidence are overalls, midrange and close-up photos. When taking any of these photos remember to keep the film plane parallel to the subject/object to minimize distortion.





12-4.4. A photograph can be inaccurate due to improper exposure either underexposure (not enough light) or over exposure (too much light). For critical comparison, photographs can be bracketed at a +1 or -1 exposure allowing the photo to be properly exposed. Most automatic cameras have an exposure compensation dial that will allow bracketing. There are certain instances where an improperly exposed picture is better than a properly exposed one. It may be necessary to photograph a scene the way the witnesses observed it. This may be in dim lighting or bright sunlight and the photographer may have to underexpose or overexpose the photograph.

12-4.5. There are four common exposure modes that can be set on the camera.

a. Manual Exposure Mode is when the photographer determines the camera settings. The photographer is responsible for setting the camera's f-stop and shutter speed (SS).

b. Program Exposure Mode is when the camera sets both the f-stop and SS, based on the camera's light meter reading (the light meter is usually next to the lens, on the front face of the camera). The photographer does not have to worry about the proper settings since the camera is in "automatic".

c. Aperture Priority Mode is the setting used when the photographer sets the desired f-stop and the camera chooses the appropriate reciprocal SS required to properly exposing the photograph.

d. Shutter Priority Mode is the setting in which the photographer sets the desired SS and the camera will select the reciprocal aperture required to properly expose the photograph.

12-4.6. An electronic flash is designed to be the same intensity as the mid-day sun. This provides the right amount of light and the right quality of light for a proper exposure. At different distances, the flash will have a different intensity. When using an electronic flash, the first thing that must be done is set the flash unit to the corresponding ISO film speed being used in the camera. The flash has a small sensor eye located on the front of the unit that measures the amount of light reflected from the scene. The flash determines when enough light has been

reflected for a proper exposure and can actually cut short the flash duration to prevent over-exposures.

12-4.7. The purpose of crime scene photography is to document the scene and evidence found at the scene. Photographs provide:

a. A permanent visual record of the overall scene

b. Mid-range photographs will depict the relationship of the evidence to the scene

c. Close-up photographs will depict the significant items at the scene

d. Photographs may help determine investigative leads to pursue.

e. Photographs will assist in helping refresh memory while undergoing testimony and clarifying issues during trial

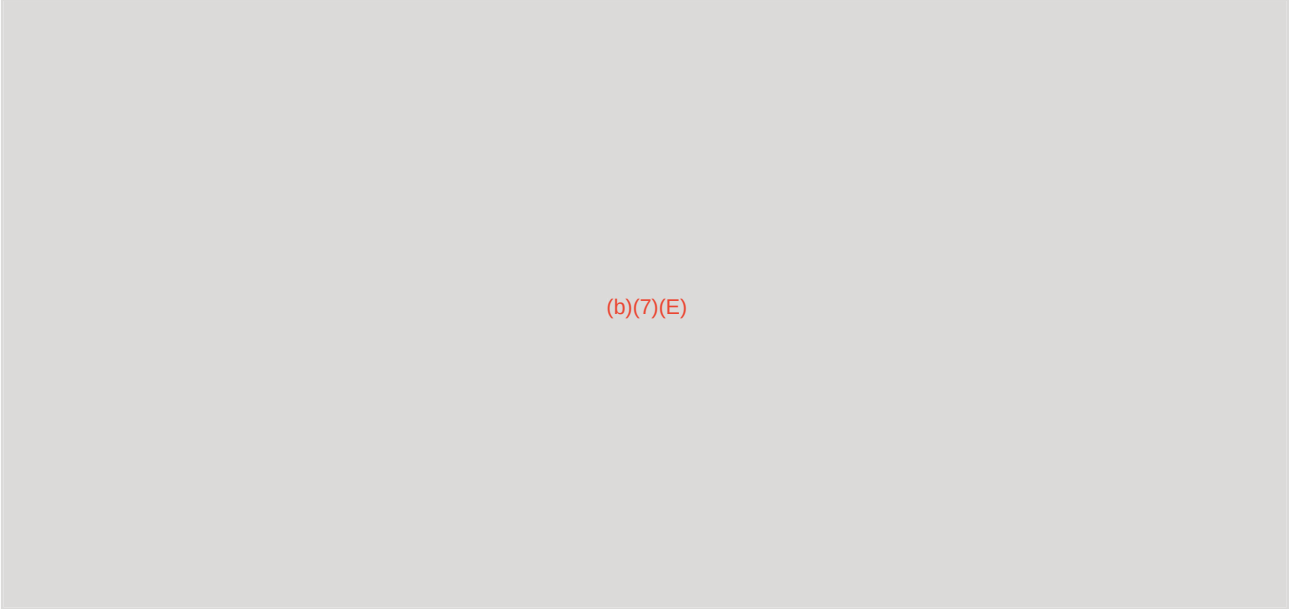
12-5. CRIME SCENE SKETCH

12-5.1. Necessity For Sketch. The scene of a crime frequently reveals many clues that assist the investigator in the solution of the crime. Coincidental with the procedures of protecting the area of the crime from contamination or alteration by interested bystanders is the employment of a specialized technique known as a crime scene sketch wherein the preservation of the crime scene is maintained for thorough study and possible detection of physical evidence. This sketch, a graphic representation of a scene depicting essential details, may be used to supplement photographic coverage in a more valid and realistic manner since photographs do not provide exact measurements of distances between objects nor determine the precise sizes of such objects. Certain objects, moreover, are not visible in a photograph or cannot be clearly identified. A drawing, or crime scene sketch, is the simplest and most effective way of showing actual measurements and identifying significant items of evidence in their location at the scene. In sketching crime scenes, the investigator shows the scene, specifies where evidence is found, and shows objects and their relationship to one another, and outlines approaches or entrances to other structures. Sketches, in addition to supplementing photographs, support, clarify, and augment written descriptions. Sketches may be either rough draft sketches or finished drawings. These serve to outline the evidential facts in an investigation by fashioning a clear reconstruction of the crime scene.

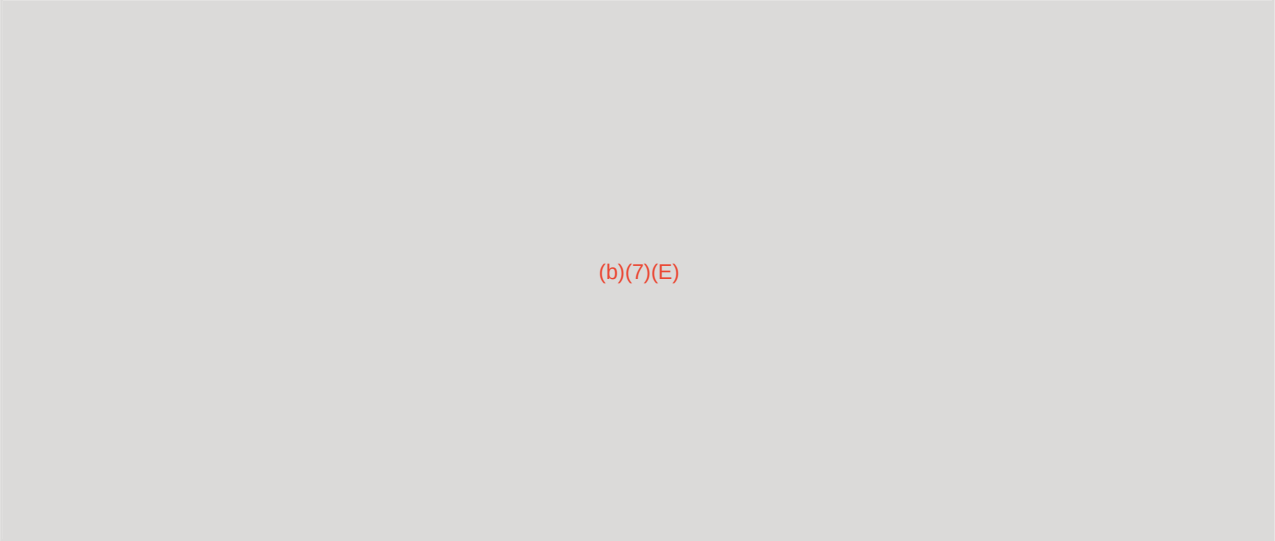
12-5.2. Materials. Sketch materials should be readily available in a portable kit. Sketch equipment might include nothing more than a paper pad, ruler, protractor, pencils, and magnetic compass; however, more advanced equipment utilized in either mechanical or architectural drawing may complement the basic kit and prove invaluable to the agent.

a. For the rough sketch at the scene of the crime, it is generally desirable to use a soft pencil and graph paper. Graph paper is excellent for sketching as it provides a guide for lines and proportions. A clipboard can serve as a sketching surface. A compass to indicate proper orientation of the sketch and a tape measure to record accurate measurements should be used.

b. For the finished drawing, the agent draftsman will require a drawing set, a drafting board with accessories, ink, and a good grade of drawing paper. A finished drawing is a specialized refinement of the rough draft sketch, by a person skilled in mechanical or architectural drawings, and made usually for courtroom presentation as well as being utilized as an appropriate enclosure to the agent's report. Computer assisted drawing/design (AutoCAD) programs are also commercially available and investigators can utilize them to prepare diagrams simply by inputting measurements.



12-5.4. Categories of Sketches. Investigative sketches are divided into three types: locality, grounds, and details:



12-6. GENERAL RULES FOR SKETCHING

12-6.1. The following rules should be heeded when sketching crime scenes. Please remember that sketching should be done for all scene examinations and is required for all death scenes:

(b)(7)(E)

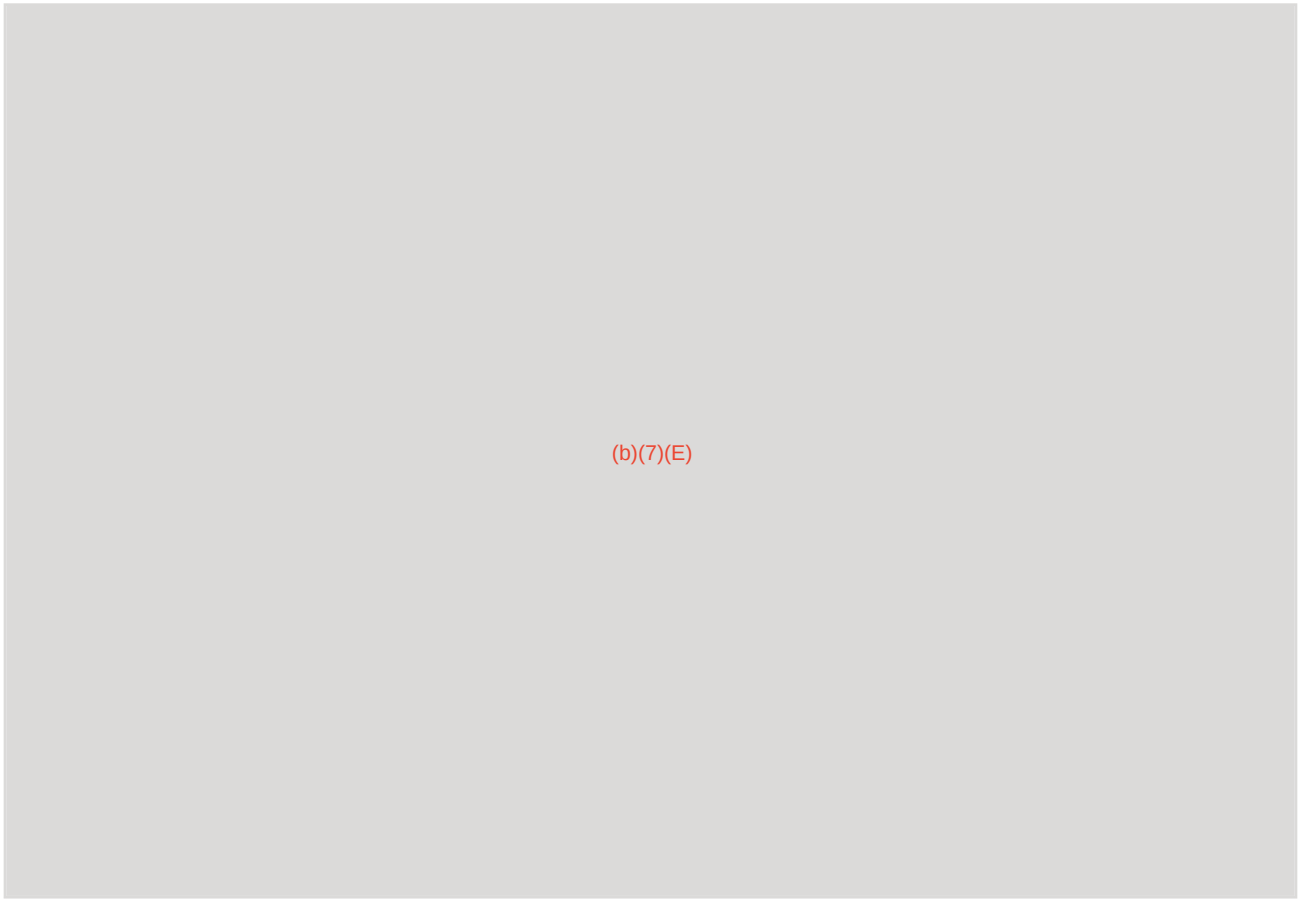
12-7. CRIME SCENE NOTES

12-7.1. The notes of the investigator at a crime scene are his/her personal and most readily available record of participation, observations during the crime scene search, and time spent at the crime scene. While it is obvious that the more detailed the notes are the more valuable they become, it would be impractical to attempt to formulate a rule regarding detail content of the investigator's notes. The objective of crime scene note taking, however, is simply stated. The notes must be logical and written so that they will remain meaningful months after the incident. Notes should also be dated/initialed and contain title/CCN information.

12-7.2. The taking of crime scene notes should commence with the investigator's assignment to the case and continue through the completion of the investigation. They should be recorded in chronological order of observation; which means at this stage of the recording process they will not necessarily be in logical order since it is important only that the notes are complete. The investigator will later reorganize the information during the formal report writing.

12-7.3. The following are the essential elements of information to be covered in the investigator's notes. This listing is not intended to represent all of the categories of data that may be useful and which may be recorded:

(b)(7)(E)



12-7.4. Notes are valuable, not only as an aid to accurately recall of events to be testified to in court, but also to furnish the raw material for the written report of the case. (b)(7)(E) (b)(7)(E) The details recorded during the investigation should anticipate both the written report requirements and the possibility of the special agent being questioned on a given point by attorneys or the court. Unless a different notebook is used for each case, a loose-leaf notebook is preferable to a bound notebook. If notes from several investigations are included in the same book and the book is subsequently examined in court, there is a possibility of unauthorized disclosure of information concerning matters not being dealt with in the case being heard. If a loose-leaf notebook is used, the pages applicable to a case can be removed and the possibility of unauthorized disclosure of facts relative to other cases is avoided.

12-7.5. The investigator's notes relative to a search should be secured in a safe place until such time as the case is closed. They should then be retained with the NCISRA case file pending exhaustion of all possible judicial administrative action. Even if the suspect is convicted, there is always the possibility that an appeal will require the investigator's reappearance in court; like physical evidence, the notes should be retained until such time as appeal avenues have been exhausted.

12-7.6. In major cases where the amount of physical material is large and search of the crime scene is very lengthy and involved, a portable recording device may prove valuable. By

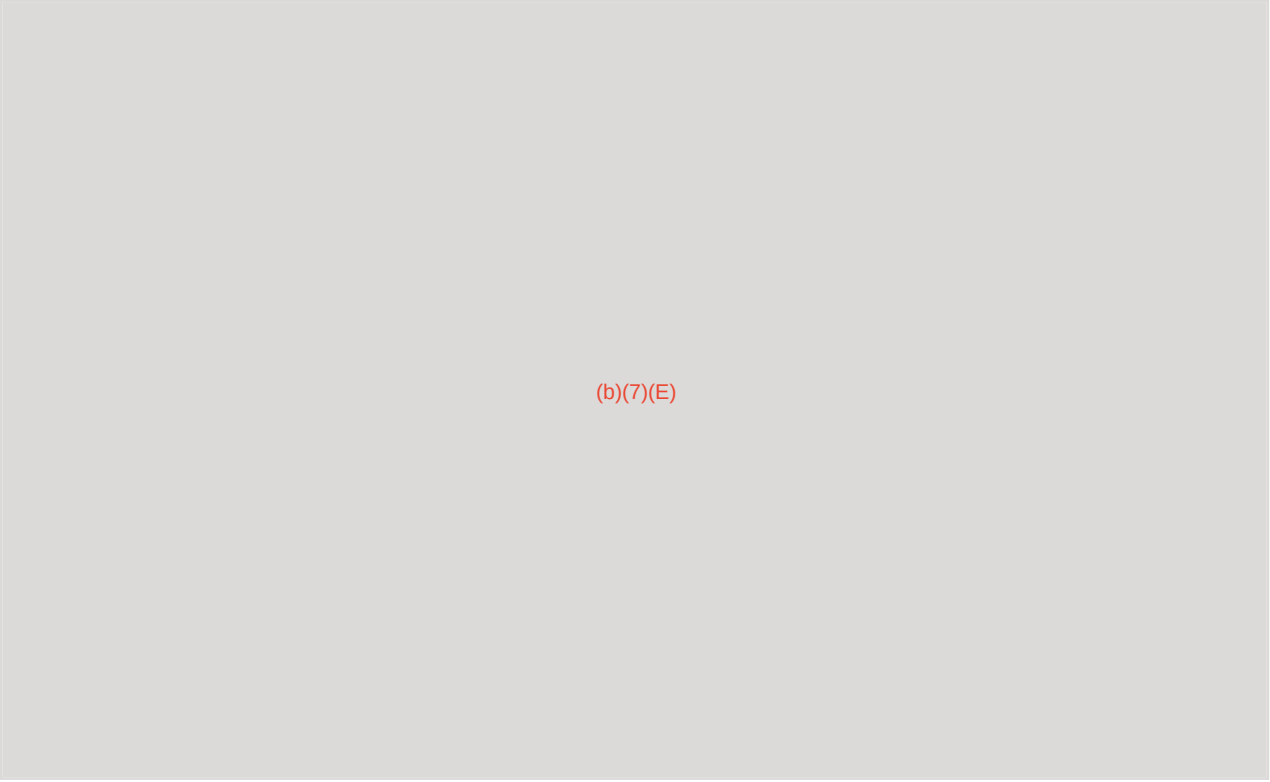
recording observations and findings, the investigator can include more data in the notes. During this process, the investigator should refrain from making any off color remarks, and encourage colleagues to do the same. One does not want to cause the agency undue embarrassment if the recording were to become available for trial. When the investigative recording is complete, the tapes should always be transcribed into a written record for the investigator's use in court.

12-8. DETAILED SEARCH OF THE SCENE

12-8.1. Excluding the unforeseen, the crime scene should be recorded before any objects are collected or removed from it, with the obvious exception of medical assistance to injured persons.

12-8.2. Various crime scene-searching techniques have been suggested, recommended and utilized by criminal investigators. Regardless of the technique used, the basic objective of the search is to locate physical evidence and witnesses to the crime under investigation. Whichever search technique is decided upon, ensure that all investigators are utilizing that same search technique to prevent unnecessary searching. Everyone must work together to ensure that all areas of the scene are searched so that no evidence is missed. Additionally, the circumstances of the case must always govern the investigator's actions in processing the crime scene. Experience has shown that the following general rules are useful in helping to systematize the search and to prevent error:

a. One must triage the evidence. Evidence that is being significantly deteriorated by time or the elements has first priority.



(b)(7)(E)

12-9. TRACE EVIDENCE

12-9.1. Dust, dirt and debris associated with a crime scene is referred to as “trace evidence.” (b)(7)(E)

(b)(7)(E)

Page 341 redacted for the following reason:
- - - - - - - - - - - - - - - - - - - -
(b)(7)(E)

(b)(7)(E)

12-9.2. Trace evidence may either be left at or carried away from the scene of a crime by either the perpetrator or victim. The intrinsic value of trace evidence depends on how nearly it falls into one of the following categories:

a. Common and/or widespread matter has some individuality or characteristic. *Example*:

(b)(7)(E)

(b)(7)(E)

12-10. TOOL MARKS

12-10.1. (b)(7)(E)

(b)(7)(E)

(b)(7)(E) If an article bearing marks or impressions cannot be moved, appropriate cast and mold procedures should be undertaken as prescribed in NCIS-3, Chapter 11. Under no circumstances should the investigator attempt to fit a suspected tool into a tool mark. Such an action could obliterate some of the characteristic impressions and striations of the tool mark.

12-11. FIREARMS EVIDENCE

12-11.1. In connection with certain types of crime, firearms evidence found at the scene of the crime will be of utmost importance and value to the investigator in solving the crime and, likewise, of extreme value to the prosecutor at the trial of the criminal. However, unless the firearms evidence that is obtained during the investigation is properly handled and properly packed, its value may be reduced considerably.

12-11.2. (b)(7)(E)

(b)(7)(E) The firearms may be a pistol, revolver, shotgun, rifle, machine gun or some other type of firearm. Each type of firearms evidence obtained will require its own special method of handling because of the type of laboratory examination that may be required.

12-11.3. Safely collect firearms by ejecting any rounds within the chamber and if a magazine is present, removing it as well. In the case of revolvers (b)(7)(E)

(b)(7)(E) Do not remove rounds from the magazine. To package firearms, place the weapon diagonally inside a box with the end of the barrel in one corner and the stock or handle in the opposite corner. Ensure that the weapon is securely in place. (b)(7)(E)

(b)(7)(E)

12-11.4. Should the evidence be in the form of a spent bullet, or a fatal bullet, extreme care must be exercised in handling it. (b)(7)(E)

(b)(7)(E)

Pages 344 through 345 redacted for the following reasons:
- -
(b)(7)(E)

(b)(7)(E)

12-13.4. Standards should always be collected before the crime scene is released, as the investigator can never depend on being able to return for such material. Decisions concerning which material is valuable as a standard are largely dependent on the investigator's experience and judgment; when in doubt, collection of excessive samples is the wisest course.

12-14. FIRES AND EXPLOSIONS

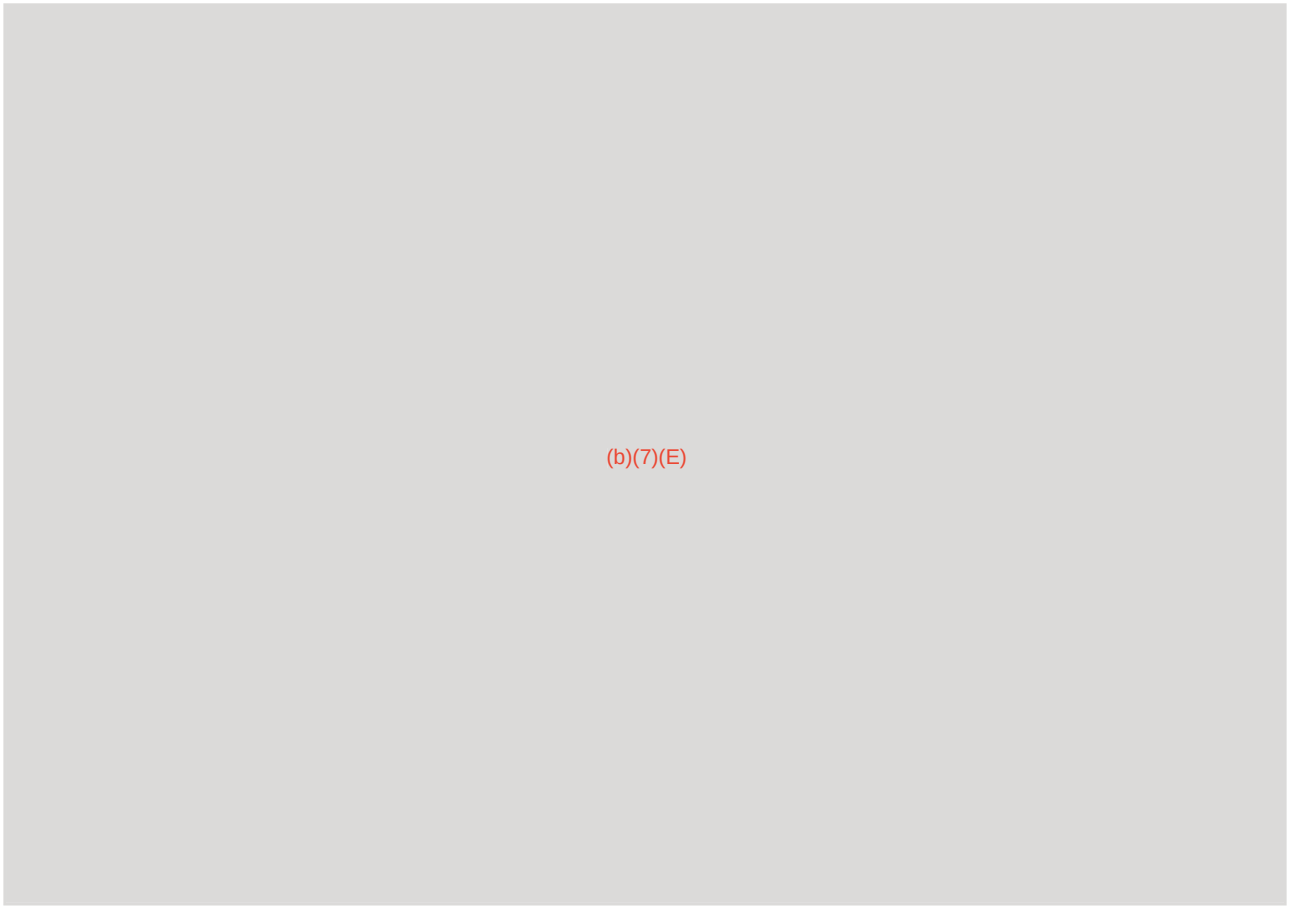
12-14.1. The fire or explosion scene is processed in much the same way as other indoor crime scenes insofar as the protection and preliminary stages are concerned. (b)(7)(E) (b)(7)(E) (b)(7)(E) The detailed search, however, involves some special considerations and problems to include the following:

a. The structural integrity may have been severely weakened. Take measures to avoid a structural collapse.

b. There may be explosive devices that did not detonate. Such secondary explosives may have malfunctioned, or they may be intended to target scene response personnel. If an unexploded device is located, do not attempt to disarm the device yourself. Evacuate the area and wait for a bomb disposal unit.

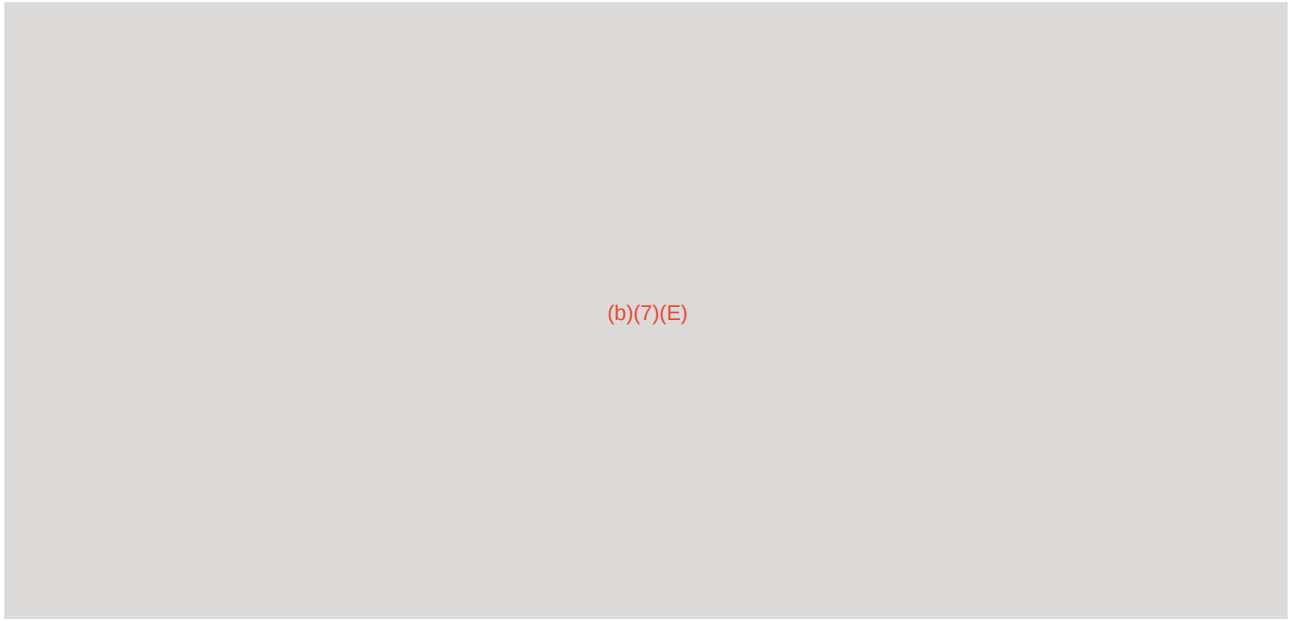
c. Also, make note of the nature of the scene. (b)(7)(E) (b)(7)(E) (b)(7)(E) The basic problem facing the investigator in a fire and explosion is to determine if a crime has been committed.

(b)(7)(E)



12-14.6. The foregoing comments primarily concern elementary observations to be made in connection with searching the scene of a possible or suspected arson/explosion. Additional, detailed guidance is contained in NCIS-3 Chapter 25, Bomb and Arson (Category 6A).

12-15. SEARCHING THE OUTDOORS



(b)(7)(E)

12-16. VEHICLE SEARCHES

12-16.1. Detailed searches of vehicles must be as carefully planned and systematically carried out as those for indoor and outdoor crime scenes. The nature of the investigation will dictate how detailed the search must be. (b)(7)(E)

(b)(7)(E)

Pages 349 through 350 redacted for the following reasons:
- -
(b)(7)(E)

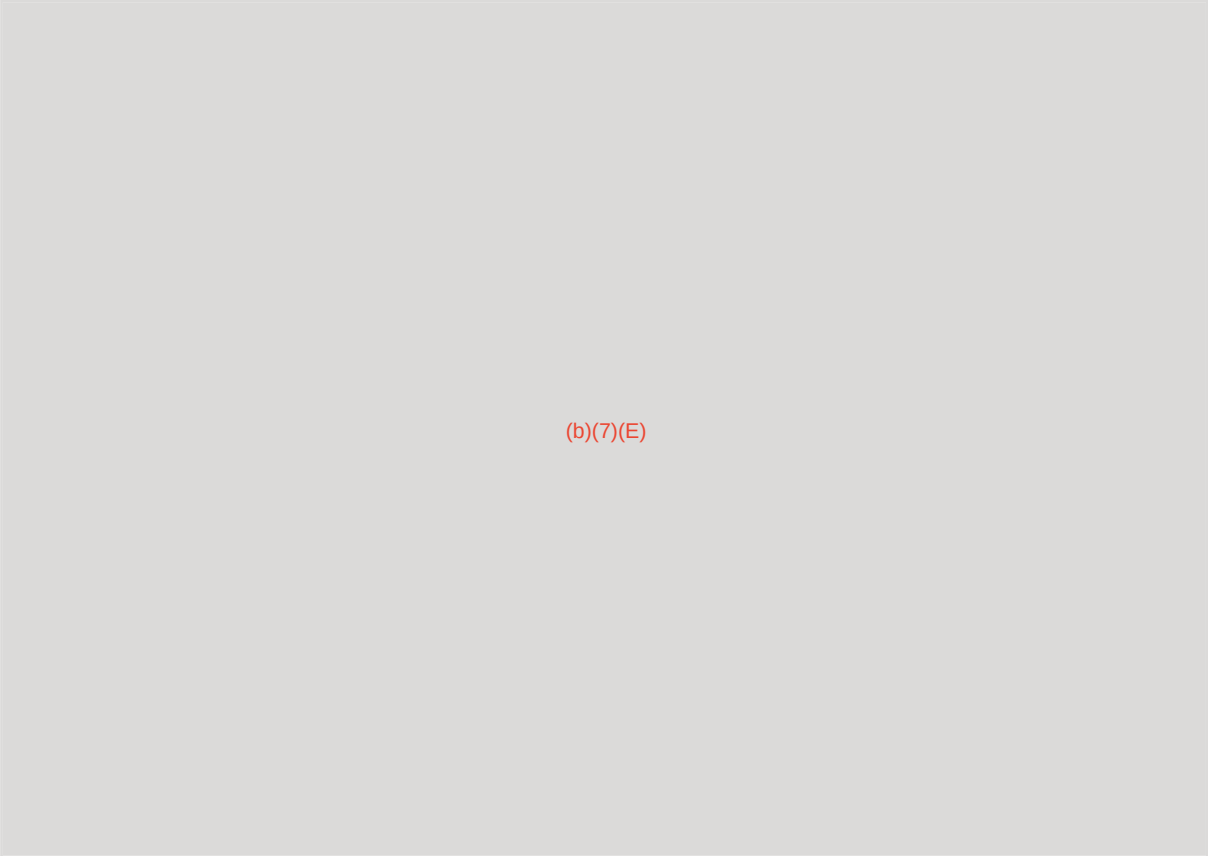
(b)(7)(E)

12-17.6. Further discussion and guidance concerning the search of a death scene and examination of the deceased is contained in NCIS-3, Chapter 30, Death Investigations**.** Of prime importance is the necessity for the investigator to consult with the forensic pathologist/physician to insure that any spent projectiles or other objects removed from the body are properly handled, marked and promptly released as evidence to the investigator for submission to the crime laboratory.

12-18. RECOVERY OF OTHER PHYSICAL EVIDENCE

12-18.1. Related to the acquisition of physical evidence and standards from the crime scene, and of equal importance, is the recovery or seizure of eliminating or incriminating evidentiary items from living victims and suspects. (b)(7)(E)

(b)(7)(E)



12-19. PROCESSING OF EVIDENCE FOR LABORATORY EXAMINATION

12-19.1. It has been previously discussed that consideration should first be given to the preparation and shipping of evidence to avoid contamination or other change. The second consideration is the proper identification of the evidence in such a manner that it can be recognized and adequately introduced in court. It is essential that persons handling evidence become thoroughly acquainted with the distinctive features or marks of evidentiary items in order that they can positively recognize them at a later date. Several aspects of identification handling and marking of physical evidence must be considered. The manner of identification and specific location of the item are of equal importance in marking evidence. In all instances of evidence identification, the initials of the investigator and the date and time of collection are required data that must be appropriately marked either on the item, tag, or container affixed to or enclosing evidentiary material. The markings must be in a manner that will enable the investigator to identify the item at a subsequent date, possibly several months later.

12-19.2. A partial list of suggested methods of evidence handling, marking and packaging, and a summation of the investigative value of various items of evidence, is provided as Sample (1) at the end of this chapter. In the event a particular item of evidence possesses unique characteristics, the servicing criminal laboratory should be contacted for specific instructions for transmittal of evidence to the laboratory.

12-19.3. Evidence submitted to a laboratory for analysis must be accompanied by a Crime Laboratory Examination Request form. This form will often serve as a letter of transmittal for the evidence; however, some laboratories may require a separate letter or use of their own lab examination request form. When forwarding evidence to a seat of government laboratory, one copy of the form should be forwarded to NSICHQ.

12-20. LABORATORY EXAMINATIONS

12-20.1. The utilization of scientific laboratory methods in seeking the solution of crimes is of recognized importance. Special agents should become aware of the capabilities of forensic laboratory facilities and seek their guidance and assistance. The most commonly used forensic laboratory is the U. S. Army Criminal Investigation Laboratory (USACIL) located in Forest Park, GA. Other laboratories that can be utilized if available are the FBI Criminal Laboratory, Quantico, VA and other local and state labs. When specialized or unique laboratory methods are desired, forensic laboratory personnel can be utilized in training evolutions so that special agents can be both familiar with what scientific assistance a laboratory can provide and the proper manner in which to collect, preserve, and submit physical evidence for analysis. Scientific analysis can often yield additional investigative leads; the results of which may frequently be utilized in prosecution of the case in court. Following are some of the more prominent types of forensic examination procedures:

a. Spectrography. The science of measuring the elemental wavelengths of a substance. Every substance has characteristic wavelengths that are developed by the use of the spectrograph. The principal advantage of spectrography is that results may be obtained from minute specimens. An example would be the small particles on knife blades or other tools, which could be compared with the metal from burglarized safes, dirt from under fingernails, and many other particles of evidence.

b. Microscopy. The examination of small characteristics not easily visible to the naked eye that may be unique to that piece of evidence. Common types of microscopy include:

(1) Polarized light microscopy in trace fiber analysis, when determining the refractive indices of fibers.

(2) Comparison microscopy is often used in firearm and tool mark examination.

(3) Stereoscopes are used when only slight magnification is required. Stereoscopic microscopes are also the only light microscopes that will show evidence in 3D. They are particularly useful in document examination.

(4) Petrography is the examination of minerals and soils.

(5) Scanning electron microscopy (SEM) is often used when examining gunshot residue. When viewed under SEM, the particles of lead, barium, and antimony have a unique configuration consistent only with GSR. Dust found on clothing may be compared with similar dust found at the scene of the crime. Much of this evidence is circumstantial in nature, but if the

materials share a likely common origin and represent a small portion within the general population, and are present in quantities far greater than would normally be expected, they may still be sufficient to secure a conviction.

c. Toxicology. Deals with the science of poisons. It treats the origin, nature, properties, effects and detection of poisons, and may include treatment of poisoning. Investigators may be called on to investigate deaths or sickness caused by poisoning and, in cases where death results, to determine manner of death. Poisons are divided into the following general groups:

(1) Alcohol (Wood-Methyl)

(2) Acids

(3) Alkalies

(4) Alkaloids

The general groups listed above are broken down into a large number of specific materials, such as cyanide, lead, arsenic and others. Evidence recovered during investigations of suspected poisonings should be carefully preserved. (b)(7)(E)

(b)(7)(E)

d. Glass Fragments. Broken or fractured glass found at the scene of a crime frequently furnishes important leads. (b)(7)(E)

(b)(7)(E)

(b)(7)(E)

e. Invisible Radiations. Although invisible, Infrared and ultraviolet light make it possible to examine evidence by using photographic and other technical materials sensitive to their radiations. (b)(7)(E)

(b)(7)(E)

f. Firearms Identification. A system of firearms identification has been developed making it possible to determine if a certain gun fired a specific bullet. (b)(7)(E)

(b)(7)(E)

(b)(7)(E)

g. Restoration of Numbers. Objects, which bear identification numbers, such as revolvers, knives, automobile engines and parts, typewriters and instruments, are frequently encountered in investigations. Sometimes it has been found that the numbers are not visible because the metal has been ground or beaten. (b)(7)(E)

(b)(7)(E)

h. DNA Analysis. The use of DNA analysis for identification or comparison can be requested and will sometimes be the strongest link of the suspect to the crime. If a commercial DNA laboratory needs to be utilized for timeliness during a Significant Interest Investigation, concurrence by 0023B is required. When feasible, all DNA submissions should be coordinated through USACIL, the FBI, or other state and local laboratories.

12-21. DEVELOPMENT AND IMPLEMENTATION OF THE MAJOR CASE RESPONSE TEAM (MCRT)

12-21.1. Although this chapter discusses the crime scene capabilities that all special agents should possess after completing Basic Agent Training, it was determined that a specialized crime scene team needed to be initiated to assist in many major investigations. The MCRT was developed as a concept to lend a professional approach to crime scene processing. Special agents from all disciplines are trained in additional crime scene processing techniques and are called out on all major incidences to search, locate, photograph, document, collect and preserve physical evidence.

12-21.2. The MCRT provides a 24-hour surge capability of highly trained agents and relieves the case agent of crime scene responsibilities. The MCRT is a mobile response with specialized vehicles and crime scene processing equipment that can handle a major scene in a timely and professional manner. This team can easily be adapted to execute search warrants that may involve large evidence seizures from different locations simultaneously. By utilizing a standardization of crime scene processing, the expectations of professionalism and confidence can be seen in the eyes of attorneys, judges, juries, media, seat of government (SOG) and families.

12-21.3. In concert with NCISHQ, each field office is responsible for developing and maintaining a MCRT plan that addresses the following issues: identifies the team coordinator and team members, what types of incidents the team will respond to, which vehicle will be dedicated for carrying gear/equipment, and what call out procedures will be used. Case agents

investigating complex scenes should make immediate use of the MCRT capabilities via the call out procedures. MCRT leaders are responsible for submitting MCRT Call Out sheets to NCISHQ, documenting each use of the team. When feasible, training should be provided to the MCRT on a quarterly basis and documented using a Quarterly MCRT Training Report provided by the Forensic Consultant Division.

12-22. FORENSIC CONSULTANT PROGRAM

12-22.1. The Forensic Consultant program was initiated to provide NCIS with "Masters Level" trained individuals that respond and consult on complex investigations. These individuals are highly trained and can respond with the MCRT to provide advanced crime scene processing techniques. Although they are trained in all the techniques discussed in this chapter, they are also skilled in crime scene reconstruction, blood spatter analysis, firearms trajectory, glass fragmentation and assisting in forensic autopsies. The forensic consultant should be notified any time the MCRT is called out to a scene to determine if the scene requires the direct response by the forensic consultant.

12-22.2. The Forensic Consultant not only has a responsibility to assist at any major incident but will conduct a 30 day evidence review of any evidence seized at a death scene. This review will be conducted with the case agent and if appropriate with the evidence physically present. In the case of death investigations, the case agent will contact the servicing forensic consultant within 30days of the seizure of evidence to arrange for the evidence review. Along with the evidence, the Forensic Consultant will review all scene Investigative Action documents, photographs, sketches and statements that relate to the scene. After the review, the Forensic Consultant will advise the case agent what items of evidence need to be analyzed by a criminal laboratory and what type of lab testing needs to be completed. Forensic consultants will document evidence reviews using internal communications that are provided to the case agent, his/her supervisor and the Chief of the Forensic Consultant Division. After lab analysis has been completed and the case agent has received the results, the Forensic Consultant will assist in interpreting if further investigative steps need to be taken based on the analysis. When appropriate, the forensic consultant will conduct a formal Scene Reconstruction, using physical evidence to identify the events involved in the crime and sequencing those events. The Forensic Consultant is also an excellent resource for training agents that need refresher training in crime scene processing and/or advanced training for the MCRT.

Pages 358 through 364 redacted for the following reasons:
- -
(b)(7)(E)

CHAPTER 13
TITLE: EVIDENCE CUSTODY SYSTEM
POC: Code 24B3
DATE: DEC 06

APPENDICES
(1) Long Term Submission Form NCIS Form NCIS Form 5580/59 (Rev. 12/06)

POLICY DOCUMENT

APPENDIX (2) Gen Admin 11-0028 of 26 July 2011 released NCIS Policy Document No 11-16 Operational (Retention of Evidence Having Academic or Historic Significance). Policy document 11-16 contains revised or new policy that has not been incorporated into this chapter and should be reviewed in its entirety.

13-1. GENERAL

13-1.1. All items or material taken by a special agent from a subject, crime scene, or command representative and physically removed from the presence of a subject, victim, crime scene, or command representative are presumed to be of evidentiary value to NCIS by virtue of the agent's acceptance/removal of the item. Accordingly, these items must be considered as evidence and placed on an Evidence Custody Document (ECD), receipted for, and entered into the evidence system as soon as possible. If the agent subsequently examines the item(s) or causes it to be tested/ examined by a laboratory and the item is determined not to be of evidentiary value, it may be disposed of per procedures established herein. Evidence is defined as any material seized by or surrendered to NCIS that may have probative value as to the elements of an offense or the truth of a matter being investigated. Also included in the definition of evidence is all items generated by investigative personnel during the course of an investigation having probative value, such as photographic negatives, tape recordings, handwriting/handprinting exemplars,

government and personal checks, photocopies of documents for which the original is not available, etc. Furthermore, all items submitted to forensic laboratories for analysis are considered evidence and consequently require an ECD. Exceptions to this policy are very limited. Use of an evidence custody document is not required for ten-print fingerprint cards. U.S. Treasury checks must be controlled by ECD while in NCIS custody but may be taken out of ECD control when returned directly to the U.S. Secret Service. Statements obtained from suspects, victims, or witnesses only require an ECD if submitted for laboratory analysis. It shall be the responsibility of all NCIS investigative personnel to take every precaution to preserve the integrity of evidence in its original condition.

13-1.2. Evidence is considered as having been entered into the NCIS evidence system at the time it is delivered to the evidence custodian or is deposited in a night/temporary evidence container. That entry must occur as soon as possible after collection/seizure. An item seized during the investigative process is evidence upon collection and thereby requires special handling. It is recognized that certain items of evidence seized or collected by NCIS during an investigation may not be physically entered into the NCIS system after acquisition, but the evidence record system must reflect the collection and disposition of the items. As an example, items of evidence collected at a given crime scene may be immediately transferred to another agency assuming investigative jurisdiction. Evidence collected by NCIS at locations remote from an NCIS evidence locker should be properly packaged and protected to maintain the integrity of the evidence and the system. On extended road trips, it may be practical to return the evidence to the field office by registered mail or overnight delivery.

13-2. EVIDENCE CUSTODY RESPONSIBILITIES

13-2.1. RESPONSIBILITIES OF THE SAC

The Special Agent in Charge (SAC) shall be responsible for:

a. Overall supervision of the NCIS evidence custody system within the Field Office AOR to include the Consolidated Evidence Facility (CEF).

b. Assisting supervisory special agents and evidence custodians in obtaining insufficient facilities for the proper custody and storage of evidence.

c. Review of NCIS Field Office (NCISFO), NCIS Resident Agency (NCISRA), and CEF evidence custody procedures for compliance with NCIS policy.

d. Insuring that inventories of evidence within the CEF are conducted as required by NCIS policy

e. Initiating any inquiry into circumstances surrounding improper handling of evidence or discrepancies reported or discovered during the course of inventories or inspections.

13-2.2. RESPONSIBILITIES OF THE SSA

The Supervisory Special Agent (SSA) shall be responsible for:

a. Securing the proper facilities and equipment to hold/store evidence per NCIS policy.

b. Appointing, in writing, the evidence custodian and alternate custodian. It is permissible for a qualified non-agent to be appointed as evidence custodian or alternate evidence custodian.

c. Ensuring that evidence obtained is properly safeguarded, marked, packaged, documented, stored, and promptly submitted for forensic examination when required.

d. Supervising the evidence custodian and the alternate. The SSA must participate in regular inventories and day-to-day operations of the evidence locker to the extent necessary to ensure compliance with regulations and policy.

e. Ensuring that all special agents obtain disposal authorization when evidence is no longer needed, and that all disposal actions are taken per NCIS policy.

13-2.3. RESPONSIBILITIES OF THE EVIDENCE CUSTODIANS

The evidence custodian or, in his or her absence, the assistant evidence custodian has the responsibility, which cannot be further delegated, to ensure that:

a. Evidence is properly inventoried, tagged, packaged, and marked prior to acceptance for storage.

b. ECDs are properly completed prior to acceptance for storage.

c. Evidence is properly safeguarded.

d. The Evidence Log, Active Evidence Custody Record, and Final Evidence Disposition Files are properly maintained.

e. Inventories of evidence holdings are conducted per NCIS policy.

f. Under the supervision of the SAC, evidence is disposed of properly.

13-2.4. RESPONSIBILITIES OF SPECIAL AGENTS

Special agents receiving evidence shall be responsible for ensuring that:

a. Evidence is properly:

(1) Marked for identification.

(2) Inventoried.

(3) Packaged.

(4) Tagged.

(5) Entered into the custody system or placed in designated temporary evidence storage without delay.

(6) Protected.

b. Appropriate receipts are provided when requested or required.

c. Evidence Custody Documents (ECD) are properly completed.

d. Through appropriate liaison, when stored evidence has served its purpose, an authorization is obtained for its final disposition and the evidence custodian is notified in writing.

e. Evidence obtained is returned to the proper party or otherwise disposed of per NCIS policy.

f. Evidence holdings are reviewed with Evidence Custodian 30 days prior to departure for new duty station to allow for return of evidence to owners or contact with commands.

g. Evidence required for court proceedings is checked out from the CEF and transported to the legal facility in a timely manner, securing a proper transfer of custody as set out in paragraph 13-10.2 below.

13-3. AUTHORIZED EVIDENCE LOCKERS

13-3.1. All evidence shipped to NCISHQ, for whatever reason, shall be turned over to the Washington Field Office evidence custodian for maintenance. In cases where evidence requires review by one or more NCISHQ Directorates, tasking documentation listing the required examinations will be forwarded, as appropriate, with duplicates of the tasking documents accompanying the evidence to assist evidence custodians. In addition, NCISHQ Code 22 will coordinate with the SAC Washington Field Office to appoint an additional alternate evidence custodian who will be charged with the responsibility of maintaining classified evidence requiring specialized storage and handling.

13-3.2. NCIS field offices associated with a CEF shall not establish or maintain separate evidence lockers, and NCIS components shall not transfer any such items to a field office serviced by a CEF. In the event that such a field office receives evidence from an outside organization, the evidence will be immediately transmitted to the nearest CEF for custodial purposes. The field office will, of course, prepare an ECD covering the items if the evidence has been received other than in a sealed condition.

13-3.3. Each NCISRA and Afloat NCIS Resident Unit (NCISRU) shall establish and maintain an evidence locker as described herein.

13-3.4. Other NCISRUs may have a requirement to establish and maintain an evidence locker. Only those NCISRUs authorized in writing by their respective field offices shall maintain evidence lockers. In most instances the distance from the parent field office will be the determining factor.

13-4. PHYSICAL SECURITY AND FACILITIES FOR EVIDENCE LOCKERS

13-4.1. NCIS field components, so authorized, shall maintain a designated evidence locker consisting of: one or more field safes, two-drawer (or more) security filing cabinets, safe(s), or any combination thereof. In field components where large volumes of evidence are handled, the evidence locker should be a separate "strong room." A closet may be adequate, or a larger room may be necessary. Each Cyber Unit is to have and maintain dedicated evidence storage lockers and safes consistent with the guidelines set forth in this chapter.

13-4.2. Any container utilized for the storage of evidence shall be secured with a type of lock specifically mentioned within this section. GSA-approved security containers can be without supplemental controls. Until 1 October 2012, a non-GSA approved security container with a built-in combination lock or a secure room (open storage area) can be used with one of the following supplemental controls:

a. The location housing, the security container or secure room is subject to a cleared guard or duty personnel.

b. A cleared guard or duty personnel shall inspect the area once every 4 hours.

c. An Intrusion Detection System will be installed with personnel responding to an alarm within 30 minutes of alarm annunciation.

Note 1: The secure room must meet the criteria of Exhibit 10A of SECNAV M-5510.36.

Note 2: There are several GSA-approved containers in service that do not have an X-07, X-08 or X-09 (FF-L-2740) built-in. They can still be used until 1 October 2012. Secure rooms must have a lock meeting FF-L-2740 specs built-in or you must have an exception/waiver from CNO N09N2.

13-4.3. The use of a lock bar-padlock variety of filing cabinet for an evidence container is not authorized.

13-4.4. Key locks are generally considered less secure than combination locks because of the key's traditionally greater susceptibility to manipulation, in conjunction with the problems to proper key security. The Operational Support Directorate (Code 0024B) feels these problems have been sufficiently minimized in at least one key lock to warrant authorization in lieu of the traditional combination lock. The FF-P-110 is the only lock approved by GSA for protection of classified material. Key actuated padlocks, such as the S&G 833 can be used to secure large items, such as crates, Connex boxes containing classified material, by exception (see Chapter 10, SECNAV M-5510.36).

13-4.5. If key locks are used for securing evidence, a rigorous program of key security is to be practiced. Only two keys for each lock will exist; one is kept by the SSA in a sealed envelope in his or her safe; the other's access is strictly limited to the evidence custodian, alternate evidence custodian, and supervisory special agent and is not to leave NCIS office spaces. Inventory of both keys shall be a part of each evidence inventory; satisfactory sighting shall be so noted. The cylinder must be replaced whenever compromise of the integrity of the evidence security system is established or suspected.

13-4.6. A cipher locker does not constitute a proper locking device and will not be utilized to secure NCIS evidence facilities. If the utilized container is of such weight that it can be reasonably considered removable, it shall be secured to the deck or bulkhead in such a manner that it, or the part of the structure to which it is attached, must be destroyed to remove it from the office space. If a closet or room is utilized as a strong room for evidence storage, wooden access door(s) of solid-core construction or metal doors shall be secured with one of the aforementioned locks, and the hinges on the access door placed so they are on the inside of the evidence room. If this is not feasible, the hinges shall be of such type, or so modified, that the hinge pins cannot be removed without destroying the hinges or door. Should the evidence locker (room) have windows, they will be covered with expanded steel gratings of 9-gauge thickness and securely attached to the building with fastenings or anchoring devices that are not removable without permanent destruction. The perimeter walls of such a room shall extend from the true floor to the true ceiling. Utility openings, such as ducts and vents, will be kept at less than man passable dimensions. This dimension is 96 square inches or less of an opening. Windows that are above 18 feet off the ground shall be made opaque or equipped with blinds, drapes or other coverings. When a room is utilized as the evidence locker, one or more metal locking containers shall be utilized to store high-value evidence such as firearms, large quantities of narcotics, currency, jewelry, etc. When currency is held in evidence, it shall be stored in a fire-proof container if at all possible. When a container or room has been designated as an evidence locker, other materials or equipment, personal or official, shall not be stored therein.

13-4.7. When a closet or room is utilized as an evidence locker, it should be equipped with shelves, storage bins and cabinets, lockers, or other suitable means for storing a volume of evidence in an accessible manner. Shelves, bins, or lockers, etc. shall be marked in a manner that facilitates the location of particular items of evidence.

13-4.8. Access to the evidence locker (container) will be strictly limited by the appointed evidence custodian, alternate custodian, and SSA. In the event that the alternate evidence custodian is not the SSA, the latter shall be provided the combination(s) in a sealed envelope and, if appropriate, the key or keys to all evidence containers for use when the custodian or alternate is not available. In no event shall personnel other than the evidence custodian, alternate evidence custodian, SSA, or SAC be granted unescorted access to the evidence locker. Combinations to all evidence containers should be changed whenever the evidence custodian, alternate evidence custodian, SSA, or SAC is changed. Requirements for changing combinations under various circumstances are:

- **a.** The lock is initially placed in use. Manufacturer preset combination may not be used.

b. Any person having knowledge of the combination who no longer requires access to the evidence locker (loss of clearance, transfer, etc.).

c. The combination has been compromised (unauthorized personnel having to open safe during emergency).

d. The combination has been taken out of service.

e. Repair work has been performed on the combo lock. Optional Form 89 (OF 89) is also required.

f. At least once every 2 years or sooner as directed above.

13-4.9. At each NCIS field component, provisions shall be made for the receipt of physical evidence after normal working hours or when the evidence custodian or alternate is not available. The following methods have been found to be satisfactory in varying degrees as indicated:

a. A large locked drop box, (ex. a steel, out of service, U.S. Mailbox) secured to the floor or other portion of the NCISRA/ NCISRU structure, is utilized as a receptacle with the same type of lock as the evidence locker securing it. Properly packaged evidence with ECDs attached is inserted in the drop box. The evidence custodian or alternate routinely checks to see if any material was deposited therein and, if so, transfers it to the regular evidence locker. The limiting factor with this device is the size of the material that can be inserted in the mail drop.

b. One or more small clothing or gym type lockers, secured to the structure, are utilized as receptacles. A combination lock is attached to each locker in an unlocked or open condition. The evidence, properly packaged with completed ECD attached, is placed in the locker and the combination lock is secured. The evidence custodian or alternate will subsequently remove the evidence from the locker as appropriate.

c. One of these systems will preclude evidence from being stored in various locations around the field component and the necessity of the special agent personally contacting the evidence custodian to secure evidence. In no event shall agents maintain physical evidence in their possession longer than necessary to prepare the evidence and required documentation for submission to the evidence custodian.

13-4.10. NCISRUs established afloat are exempt from the physical requirements set forth above; however, special agents assigned afloat shall make the most secure arrangements possible for the storage of evidence aboard ship, and may transfer evidence which must be held for extended periods of time to their parent NCISRA or other NCISRA as appropriate for custody. All such transfers are temporary in nature, and the responsibility for proper disposal of that evidence lies with the afloat agent. All evidence records, such as the evidence log, active evidence custody record, and final disposition file, are to remain with the NCISRU permanently or until the ship is decommissioned.

13-4.11. All NCIS components shall make every effort, within budgetary limitations, to comply with the aforementioned physical requirements for their evidence lockers. If fiscal constraints prohibit full compliance within a reasonable time, appropriate documentation shall be maintained by the component affected.

13-5. NCIS EVIDENCE CUSTODY DOCUMENT (ECD) AND EVIDENCE TAG

13-5.1. The ECD is designed to establish the necessary control and maintenance of the chain-of-custody of evidence while under the control of NCIS; however, it is not intended that any command or other agency chain-of-custody be reconstructed by utilizing this document on an after-the-fact basis. Such investigative activity shall be accomplished by obtaining appropriate statements and/or copies of other command/agency evidence documents. This does not preclude having personnel delivering evidence from marking the evidence itself or its container as appropriate.

13-5.2. If the space provided on the ECD for listing items of evidence seized is insufficient, additional item(s) must be listed on supplementary ECD, fastening the two (or more) together. If a supplementary ECD(s) is needed, the first three lines of the form(s) shall be completed in the same manner as on the first, and "Page 2" noted, etc. If there is insufficient space to document the transfer of evidence using the ECD, an NCIS ECD Continuation Sheet is to be used.

13-5.3. The NCIS Evidence Tag (NCIS 5520/119(10 0972) S/N 010509800095530) shall be utilized to identify each item of evidence obtained by NCIS and entered into the NCIS Evidence Custody System. The entries on the NCIS Evidence Tag should correspond with the applicable entries on the NCIS ECD.

13-5.4. It is recommended that appropriate collection data on all seized or collected items of evidence be entered on the evidence tag at the point and time of seizure/collection. There is sufficient space on the face of the tag to enter a description of the material, as well as date, time of seizure, and specific location where the item or material was obtained. Examples are: Parker ball point pen, seized from left shirt pocket; $10.00 note, from right pants pocket; K-Bar knife, from tool pouch in subject's auto trunk, etc. Utilization of the evidence tag in the above-described manner will provide original collection notes that can be used as: (1) a basis for creating the evidence custody document at a more convenient time and place; and (2) add to the integrity and authenticity of the evidence.

13-5.5. The NCIS ECD, Evidence Tags, and continuation sheets are stocked in the Navy Supply System, which can be procured through normal Navy supply channels as necessary.

13-6. REQUIRED EVIDENCE CUSTODY RECORDS

13-6.1. Each evidence repository within NCIS will maintain a bound Evidence Log, an Active Evidence Custody Record, and a Final Evidence Disposition File. **a.** The Evidence Log shall be maintained for a period of 5 years from the date of the last entry therein, and is presumed that it will serve for a number of years prior to starting a new volume. Atlantic and Pacific Cyber

Divisions will institute an evidence log to record all evidence that is transported into and out of Cyber Forensic work areas.

b. The Active Evidence Custody Record shall be maintained as long as there is evidence in custody that has not been finally disposed of. Once the corresponding evidence has been destroyed, the original ECD will be placed in the original case file. Ifthe case file is at NCISHQ, the ECR should be forwarded using the establishedprocedures to NCISHQ, Records Management Branch, Files Section (Code 11C12), for inclusion in the case file.

c. The Final Evidence Disposition File shall be maintained for a period of 5years after the close of the calendar year covered by the file.

13-6.2. The evidence custodian shall maintain evidence transactions only in the approved Department of the Navy (DON) evidence log (OPNAV 5527.24) available from the Federal Supply System under national stock number 0107-LF-055-2820. DCWA stocks the evidence log for HQ and local use only. Each custody document received by the custodian will be reflected on a separate logbook line regardless of how many items of evidence are listed on the document. It shall also contain date entries of all inventories, changes of evidence custodian or alternate and lock combinations. Each entry indicating a receipt of evidence by the custodian and each ECD shall be assigned an evidence log number consisting of two groups of numbers separated by a hyphen. The first number is a three digit chronological number of the document for that year, with the second group consisting of the last two digits of the year. For example, 001-07 would be used for the first evidence custody document for the calendar year 2007. If desired, additional information for local control purposes may also be entered after the above items. Each entry will be made in blue or black ink on the next blank line; no empty lines will be permitted. In the event an error is made in the entry, the line should be lined-out and initialed by the custodian. Erasures or white-outs of entries are not authorized.

13-6.3. The Active Evidence Custodian Record shall consist of copies of each ECD relating to evidence received by the custodian that has not been finally disposed of. This record shall be maintained in one or more loose-leaf notebooks, and ECDs shall be filed by Evidence Log Number with new entries being placed on top. This record will serve as a control device for periodic review of evidence holdings for possible disposal, and will represent all evidence for which the evidence custodian is responsible.

13-6.4. A Final Evidence Disposition File will be maintained of all ECDs relating to disposed evidence. This file will be kept in appropriate file folders, with one or more folders for each calendar year in which evidence is permanently disposed. The original ECD, except when it has been transferred to another investigative agency or NCIS component, shall have the final disposition section completed and be filed in the Final Evidence Disposition File by the date within the calendar year the final disposition occurred. The duplicate copy of the Evidence Custody Record shall be destroyed. In the event the original is forwarded with the evidence during the final disposition action, a copy of the original will be made and filed in the Final Evidence Disposition File.

13-6.5. The required evidence custody records shall be stored in the evidence locker in a suitable locked file cabinet or other secure container, preferably a fireproof container. Only the evidence custodian, alternate, or SSA shall have access to them.

13-7. SUBMISSION OF EVIDENCE TO THE EVIDENCE CUSTODIAN

13-7.1. When a special agent submits evidence to the evidence custodian, it shall be properly tagged, placed in appropriate containers as needed, and have the original and two copies of the ECD securely attached to the evidence or its outer container. Only the custodian accepting the evidence for entry into the system will separate the original and copies of the ECD and interleafing carbon paper. The evidence custodian shall sign, in the appropriate block, the original and all copies of the ECD to acknowledge the receipt of the evidence. The original ECD shall remain physically attached to the evidence or its container. The first copy shall be placed in the evidence custodian's Active Evidence Custody Record, and the second shall be returned to the agent turning in the evidence for inclusion in the case file. When evidence is turned into a temporary after-hours repository, the agent will sign off in the "Released by" column of the ECD after depositing the item; entering the name or number of the repository in the "Received by" column, e.g., "NFNF temporary evidence locker #3." When the seizing agent is also the evidence custodian or the alternate evidence custodian, he or she will also complete the "Released by" column on the ECD to show release by the seizing agent and receipt into the NCIS Evidence Custody System. When any evidence is checked out of the evidence locker for any purpose prior to its final disposition, a copy of the ECD shall be maintained in the evidence locker in the Active Evidence Custody Record. In the event that the original is lost or destroyed, the copy may be used in its place.

13-7.2. All evidence being submitted shall be carefully examined, counted/weighed (as appropriate), sealed (where possible) in an appropriate evidence container by the submitting agent, and verified by the evidence custodian. The submitting agent must ensure that those items being retained have some probative evidentiary value. Any items that do not have evidentiary value should be promptly returned or disposed of per authorized procedures. It is important that the ECD reflect that the described items are enclosed in a sealed container, which should also be described.

13-8. STORAGE OF EVIDENCE

13-8.1. All evidence received by a NCIS component having an evidence locker shall be stored therein, with exceptions of: evidence too bulky for storage; evidence of such a special classified nature that it requires special handling; highly perishable items such as food and human or animal parts; items of an unstable chemical or flammable nature; and explosives (see section 13-15 and 13-16 below). These types of evidence may be stored elsewhere, with the prior authorization of the SSA/SAC, where restricted physical access to the evidence can be maintained. In any event, all such items, unless of an especially bulky nature, shall be wrapped or placed in containers and sealed so that any unauthorized access to the evidence can be detected. Personnel maintaining temporary custody of the above types of materials should be

briefed on the requirements for secure storage and the probable requirement for them to testify as to their custody. Further, they should be required to properly execute the ECD upon receipt and release of the evidence. The original ECD is usually kept with the evidence unless the storage conditions may cause damage or deterioration. If the evidence custodian deems it appropriate, a copy may be substituted and the original maintained in the evidence locker.

13-8.2. The evidence custodian shall be required to affect periodic liaison with local commands to ensure that arrangements exist for the secure storage, by NCIS, of evidence that can not be stowed in the conventional NCISRA/NCISRU evidence facility, i.e., ordnance, items requiring refrigeration, oversize bulk items, etc. These arrangements shall be documented as to location and liaison contact and placed inside the cover of the Evidence Log to assist NCIS personnel in storing such items without delay. A duplicate list of these locations shall be posted on the outside of the temporary evidence ("drop box") locker. This will facilitate the proper disposal of unconventional evidence during off-duty hours when the evidence log is unavailable for inspection.

13-8.3. The NCIS Evidence Custody System can usually comply with SECNAV M-5510.36, "Department of the Navy Information Security Program (ISP) Regulation; standards for handling and storing Confidential and Secret evidence. When the evidence contains Top Secret (TS), Sensitive Compartmented Information (SCI), Special Access Program (SAP) data, or Communications Security Material System (CMS or COMSEC), or CRYPTO (whether classified or unclassified) material, additional safeguards are required. In addition to increased physical security, two-person integrity (TPI) may be required for the material (CMS or COMSEC) or special access authorizations may be needed before NCIS personnel may handle it (SCI and SAP). These national security requirements do not conflict with the purpose of the NCIS Evidence Custody System, but they can complicate the handling of classified evidence.

a. Top Secret evidence may be held if the NCIS Evidence Facility meets the requirements of SECNAV M-5510.36 for storing and handling TS material. See SECNAV M-5510.36, Chapters 7 through 10.

b. Many NCIS Evidence Facilities do not meet the requirements for Sensitive Compartmented Information Facilities (SCIFs). Consequently, when SCI material is designated as evidence, it must be "sub-custodied" to the local service Special Security Officer (SSO), who assumes all responsibility for the integrity of the evidence as well as its protection as classified SCI. Note, this local SSO must be briefed and his or her SCIF must be accredited at the same classification level of the material to be stored. This procedure is similar to that used when NCIS reporting contains SCI information. When SSO material evidence must be transferred for any reason, the chain of custody can be maintained while shipping the item through the SSO (using the Defense Courier Service).

c. SAP information generally will not be made available to NCIS for entry into evidence due to the very sensitive nature of the information. Even access to the potential evidence is strictly controlled. When it becomes necessary to seize SAP material, prior coordination with NCIS Codes 22/11A is essential. The only approved communications method is via secure telephone conversation. Do not put suspected or potential SAP information into message traffic, no matter

what the classification level. This restriction does not apply to NCIS internal SAP/Codeword Program Tiger Collar (formerly Tightdoor), which may be transmitted within the NCIS system via STU III ProCom.

d. COMSEC or CRYPTO material seized as evidence in the course of an NCIS investigation requires special handling and protection not afforded other evidence. In all instances, NCIS must comply with the NSA policy and procedures for handling and controlling this highly sensitive material, as outlined in EKMS. Even unclassified COMSEC and CRYPTO materials are subject to stringent controls. The SAC, evidence custodian, and alternate evidence custodian must be aware of this contingency and, through prior coordination with a local EKMS account, establish clear procedures whereby any seized COMSEC or CRYPTO materials are transferred under evidence sub custody to the EKMS account manager, who will provide the material with the required security and protect the authenticity of the physical evidence. If there is not an EKMS account in the local area, procedures should be coordinated with the Naval Communication Security Material Systems (NCMS), ATTN N3, 1560 Colorado Ave Room 126, Andrews AFB, MD 20707-6108. When COMSEC material evidence must be transferred for any reason, the chain of custody can be maintained while shipping the item through the EKMS Manager.

e. When a security or classification review of classified evidence is necessary, forward copies only, never the original evidence, to NCIS Headquarters Code 24E (info copy to 0022), for review by the Chief of Naval Operations (N09N2/NCIS Code 24E).

13-9. INVENTORY OF EVIDENCE

13-9.1. The receiving agent must inventory the evidence when it is first received into custody from a NCIS special agent, whether confiscated during an investigation or received from another agency or command representative. The receiving agent may not rely on an inventory by the person from whom the evidence is received. Subsequently, when evidence is transferred between agents for any reason, the receiving agent must verify the inventory, unless it is received in a sealed condition. If transfer of custody is not accompanied by an inventory but is based upon intact seals, notation to this effect should be made on the evidence custody document.

13-9.2. The contents of each evidence locker/facility shall be inventoried annually. An additional inventory may be required when any of the following are replaced: evidence custodian, the alternate, the supervisory special agent, or the special agent-in-charge, if that individual is not the alternate. The new custodian should also change the combination on all evidence containers. If an inventory required by the replacement of one of those four principals occurs within the following calendar year, it may be substituted for the normal annual inventory requirement. Remote NCISRUs staffed by one special agent, will also be inventoried annually. It may be convenient for NCISRU inventories to be conducted concurrently with visits by NCISRA or field office personnel. Field elements may now do the evidence inventory to coincide with the Office of the Inspector General, NCIS Code 00I requirement to conduct an annual "self-inspection."

13-9.3. When an inventory is conducted, it shall be accomplished by the evidence custodian and a special agent other than the alternate evidence custodian. The SAC or his or her delegate

(ASAC, SSA, or other GS-13, if assigned to the field office) shall participate in the annual inventory to the extent required to make an informed judgment that the operations of the Evidence Facility, and the on-going inventory, are properly conducted. The evidence custodian and the parent field office's SAC, ASAC or other GS-13 appointed by the SAC shall accomplish inventories of Consolidated Evidence Facilities. An entry shall be made in the evidence log reflecting the inventory and the participation of the SAC or his or her delegate. Delegation of the inventory participation requirement by the SAC does not relieve that individual's personal responsibility for the operation and maintenance of the evidence system. It is a good management practice for the SAC/SSA to be personally involved in the operation of the evidence locker and annual inventory.

13-9.4. The evidence custodian will review the active evidence custody record with each special agent at least bi-monthly in order to identify evidence that may logically be considered for disposal. It shall be the responsibility of the special agent placing the item(s) in evidence to obtain appropriate disposal authority. In the event of the originating agent's transfer or termination, the SSA will be required to obtain proper disposal authority. It is recommended that an evidence review be conducted quarterly. Acopy of the ECD contained in the case file provides a ready reminder that there is retained evidence associated with the case. It is a requirement that the case file be retained in the NCISRA as long as there is evidence held. If a determination is made that the case file can be destroyed because no further action is contemplated, there may be no reason for retaining the evidence and authority should be sought for disposition of that evidence. For unresolved cases, the evidence should be retained for the period of the statute of limitations. However, in situations where such evidence will be retained for a relatively long period of time, a close review of the material should be made to ensure its evidentiary value.

13-9.5. The inventory required, at a minimum, shall consist of a reconciliation of the Evidence Log against the Active Evidence Custody Record, and a visual accounting of each item or container for which there is a log entry and no final disposition has been made. The only exception to this sighting requirement is evidence that has been temporarily transferred to another activity according to the Active Evidence Custody Record. Evidence stored outside the NCISRA/NCISRU evidence locker because of its bulk, classification, or special nature (e.g., frozen foods, explosives, etc.), shall be sighted at each inventory, as it is not considered to have been temporarily transferred.

13-9.6. When an inventory is complete, the date and reason(s) for the inventory, by whom accomplished, and the results shall be entered as the next entry in the Evidence Log and signed by both parties.

13-9.7. If the inventory is a relieving inventory, the log also shall reflect that all combinations were changed on all locks associated with evidence custody. Any discrepancies will be listed by log number and type of evidence. In the event that discrepancies are found, the evidence custodian immediately shall report them to the SSA, who will promptly report them in writing to his or her parent field office. The field office, upon being notified of any discrepancies in the accountability of evidence, shall initiate appropriate inquiry into the matter and notify NCISHQ Code 00I. The signing of the evidence log by both the evidence custodian being relieved and the

new evidence custodian, attesting to the fact that they have completed a visual sighting of each item or group of items of evidence and have found no discrepancies, will complete the transfer of all evidence held at the NCISRA/NCISRU. This negates the need to record the transfer of evidence between evidence custodians on each ECD held within the system.

13-9.8. During semi-annual visits to their components, field office personnel will conduct a review of the evidence custody system and test evidence custody procedures by reviewing selected items of evidence, the associated documentation, and a sample of final disposition actions. On the occasion of inspections of the field office or NCISRA by senior elements of NCIS, the inspectors will similarly test the system. These checks will not be considered as a substitute for the annual inventory.

13-10. TRANSFER AND SHIPMENT OF PHYSICAL EVIDENCE

13-10.1. Physical evidence coming into the possession of NCIS will at times require transfer and shipment from the NCIS component holding the evidence to another NCIS component or another agency where the chain of custody must be maintained.

13-10.2. TEMPORARY TRANSFER OF EVIDENCE TO ANOTHER AGENCY.

The original ECD will accompany the evidence when it is necessary to transfer evidence to another agency on a temporary basis, normally for laboratory examination purposes. The evidence custodian, prior to the release of the evidence, will sign the original and duplicate ECD, placing the signed duplicate in the loose-leaf notebook in the evidence locker. Those persons handling the evidence prior to its return to the evidence custodian will complete the appropriate blocks in the accompanying original ECD. A receipt must be obtained from the agency, normally a crime lab or law center, that provides for proprietary control of the evidence while it is not in the possession of NCIS. In those cases where registered mail is not used and the transfer is made by hand, a suggested method is photocopying the original custody document and obtaining a signature from the person receiving this evidence. The copy is then returned to the evidence custodian to be attached to the evidence document in the active evidence custodian record. If only part of the evidence is temporarily transferred, the original ECD will accompany that part with appropriate notations in the item column to the left of the transferring signature. A duplicate of the original ECD will be reproduced and attached to the balance of the evidence maintained in the evidence locker. Upon return of the original ECD, the duplicate may be destroyed, and a new copy of the original made and placed in the Active Evidence File. NCIS field components requiring laboratory examination of evidence at a Washington, D.C., area laboratory should mail/ship evidence directly to the laboratory concerned, not via NCISHQ.

13-10.3. PERMANENT TRANSFER OF EVIDENCE TO ANOTHER AGENCY.

If it is necessary to transfer evidence permanently to another agency assuming jurisdiction of the investigation (counterfeit currency, illegal firearms, etc.), the original ECD will accompany the evidence and will be signed out of the evidence locker by the custodian. A copy of the original ECD will be made for the Evidence Custody Record, and the agency representative receiving the evidence will complete the final disposition portion. The appropriate disposition entry will also

be made in the bound Evidence Log Book. The copy of the original ECD will then be filed in the Final Evidence Disposition File. If the agency receiving permanent custody of evidence in a case does not accept all the evidence listed on the evidence custody form, the original evidence custody form will be retained with the balance of the evidence in the evidence locker. The agency representative shall take receipt for that portion of the evidence taken, by an appropriate entry on the form, and be provided a copy of the original form. The final disposition of the evidence will not be entered in the bound Evidence Log until all evidence listed in the Evidence Custody Document form has been disposed of.

13-10.4. TRANSFER OF EVIDENCE BETWEEN NCIS COMPONENTS.

Direct transfer of evidence between any two NCIS components authorized to maintain evidence lockers is permissible, e.g., NCISRA to NCISRA, NCISRA to NCISRU, NCISRU to NCISRU. When evidence is transferred within the NCIS Evidence Custody System from one component to another, the transfer of evidence between components should be documented by ROI when the new location is other than that cited in a previous ROI. When evidence is transferred to another authorized NCIS component, the original ECD will be transmitted with the evidence. If only part of the evidence is transferred for use in court, the original will be forwarded and a copy attached to the balance. If it is known prior to transfer that the part of the evidence being transferred will not be used in court and that remaining will probably be so used, the original ECD will be retained and a copy shall be forwarded with the evidence. The NCIS component receiving the evidence will continue to use the custody document received from the other NCIS office. The item(s) of evidence will be logged the same as any others, including the assignment of a new evidence log number. The entry in the evidence log will show the new number followed, in parentheses, by the code of the originating component and the number it had assigned to the item, e.g., 085-07 (LE 092-06). The new number will also be placed on the custody document just above the original number. The receiving component will then reproduce a copy of the ECD and place it in its Active Evidence Custody Record. The component that transferred the evidence, if all evidence was transferred, will remove its copy of the ECD from its Active File, appropriately annotate the disposition portion, and place the document in the Final Evidence Disposition File. In the event that the intra- NCIS transfer is of a temporary nature, the sending component will handle its documentation in the same manner as a temporary transfer, such as to a crime laboratory.

13-10.5. In many instances it will be possible to deliver evidence by courier or messenger. This is the most secure method and should be utilized as often as possible.

13-10.6. Evidence that is mailed to another NCIS component or another agency must, in all cases, be registered with a return receipt requested. The return receipt will be stapled to the evidence document copy in the active evidence custody record. In the event the transfer is permanent, the receipts will become a permanent part of the system by inclusion in the final disposition file with the document. If the evidence is returned to the original component, the receipt will be destroyed. Certified mail or special handling will not be utilized. When evidence is prepared for mailing, it should be double wrapped with the inner wrapping marked to indicate the presence of evidence, and the package must be specifically addressed to the evidence custodian. A suitable inner marking would be

"CONTAINS EVIDENCE."

13-10.7. Normally the only other method that may be considered for shipment of evidence is overnight express shipment. This method provides a reliable system through which shipments may be tracked. If selected, the same type of inner and outer wrapping protocol should be utilized as with mail evidence transfers. If possible, rail and truck shipments should be avoided due to the lack of accountability/ security inherent in such methods. The final tracking information should be obtained to include the signer at the final destination and treated as a return receipt.

13-10.8. All NCIS components that may receive evidence by mail should instruct the mail or receiving personnel that as soon as the presence of evidence is apparent, the wrapping should not be disturbed and the package should be promptly delivered to the evidence custodian. In no event should mail or receiving personnel other than the evidence custodian tamper with the wrapping.

13-11. REQUIRED AUTHORITY FOR FINAL DISPOSAL OF EVIDENCE

13-11.1. Approval for the final disposal of evidence shall be obtained from appropriate authority. Once it is complete, it should be forwarded to the requesting/appropriate authority along with the ROI that reflects the seizure of the evidence listed in the letter. The letter's reverse side (page 2 of the sample) provides for a return endorsement from the recipient/appropriate authority. (NOTE: It is recommended that local reproduction of the form letter be on legal length paper to ensure adequate space for itemizing evidence.)

13-11.2. Normally, any evidence utilized in any court action shall not be disposed of until the initial trial and subsequent appeals have been heard and settled. Authorization for disposal must be obtained from the Staff Judge Advocate handling the original trial or the Staff Judge Advocate of the next senior command. If the evidence was utilized in federal, state, or other civilian court, the authorization must be obtained from the appropriate prosecuting attorney prior to disposal. When authorization for disposal is received, the evidence custodian shall complete the final disposition section of the ECD by recording the name and title of the person authorizing the disposal and the authorization date.

An alternative method for authorization to dispose of evidence is to contact Code 00L at NCISHQ for a determination of the status of any court-martial that is being reviewed by the Navy-Marine Corps Court of Criminal Appeals.

13-11.3. Any evidence that was utilized in any administrative process shall not be disposed of until all appeals or reviews of the initial action are complete. Prior to disposal of such evidence, authorization shall be obtained from the Judge Advocate or Command Legal Officer of the command with cognizance over the person against whom the action was taken. In the event of their absence, the next senior command should be contacted. When authorization is received, the evidence custodian shall complete the final disposition section of the ECD, indicating the name and title of the person authorizing the disposal and authorization date.

13-11.4. Any evidence entered into the NCIS Evidence Custody System not utilized in a judicial or administrative action, may be disposed of after 6 months. Exceptions to this procedure must be made in significant unresolved cases where the evidence should be retained until expiration of the statute of limitations. An example might include lifted latent fingerprints. The SAC may authorize such disposal after appropriate consultation with the affected command. In such cases, the evidence custodian will complete the final disposition section of the ECD setting forth the SSA as the authorizing authority.

13-11.5. Evidence entered into the NCIS system and pertinent to individuals assigned to ships scheduled for decommissioning, bases that may be closed, or units that may be disbanded, must be disposed of per the foregoing procedures. Obviously, all evidence that can be returned, either to the command, subject(s), or victim(s), should be returned prior to the disestablishment of the command. In those instances where the evidence must be retained pending either judicial or administrative review, it is necessary to ensure the gaining command becomes cognizant of the evidence and the requirement to subsequently furnish appropriate disposition instructions.

13-12. DISPOSAL OF EVIDENCE

13-12.1. All evidence entered into a NCIS component's evidence locker shall be disposed of in a timely fashion, after authority for disposition is received, per the following guidance:

a. Evidence obtained during the course of an investigation that is the personal property of an individual shall be returned to that person whenever possible, with the exception of contraband items. Such items would include narcotics, unlawfully obtained drugs, illegal firearms, explosives, counterfeit U.S. or foreign obligations, or counterfeit identification. When personal property is returned to the owner or authorized representative, the individual receiving the property shall be required to sign for it in the disposition section of the original ECD or, in its absence, the duplicate copy. If the owner or his or her representative presents a NCIS property receipt when mailing his or her claim, the receipt shall be obtained and destroyed. In the event that the owner refuses to accept all the property seized, this shall be noted on the evidence custody document and other appropriate disposal shall be made of the property. In the event certain personal property, the possession of which is prohibited by command or base regulations, is entered into the NCIS Evidence Custody System, the property shall be returned to the command having control over the individual from whom it was obtained when it has served its purpose. It shall be necessary for that command to receipt for the property and make a determination as to its disposition.

b. When evidence has been received that is the custodial responsibility of a command affected by the investigation, it shall be returned to a command representative and that individual shall be required to receipt for it in the final disposition section of the ECD when no longer required by NCIS.

c. All U.S. Government property that cannot be identified as belonging to a particular activity or command shall be submitted to the nearest USN/USMC supply activity per current USN/USMC procedures. In addition to any documentation required by the receiving activity,

the activity's representative shall receipt for all the material in the final disposition section of the ECD. In the event that the activity declines to receipt on the NCIS ECD, a suitable receipting document shall be obtained and attached to the ECD.

d. Currency that cannot be returned to the rightful owner shall be turned over to NCIS Headquarters Comptroller, Code 14B2. Cash cannot be sent and will need to be converted to a check made out to DFAS-CL8522. A copy of the ECD must be attached.

e. Evidence that, by its nature, cannot be returned to the owner or entered into U.S. Navy supply channels for disposal, such as narcotics, illegal firearms, child pornography, or other contraband, shall be destroyed. The SAC, in each instance, shall authorize destruction of evidence when necessary, after other appropriate disposal authorization is obtained. Such destruction shall be accomplished by or in the presence of the evidence custodian or his or her alternate and one other impartial agent, or another trustworthy individual, both of whom shall sign the final disposition section of the ECD. Note: As the SAC has ultimate responsibility for field office AOR Custody System, he or she may not be considered a disinterested party. Also, the immediate supervisor of the CEF employees cannot be considered a disinterested party.) Such destruction shall be of a nature so as to make the evidence unusable for any lawful or unlawful purposes other than residual scrap.

f. The disposition of Emergency and Extraordinary Expense Funds (formerly Collection and Classification of Information Funds (C&CI)) held as evidence requires specific action by the evidence custodian as set forth in Chapter 37 of NCIS-1. When EEE funds are no longer required as evidence, they must be returned to the agent cashier. The evidence custodian must take the cash to the agent cashier or to a Disbursing Officer who will issue an "exchange for cash" check which will be mailed to the agent cashier. The evidence log number will be annotated on the face of the check or noted on the covering correspondence. Cash shall not be mailed nor shall the money be deposited in a personal checking account and a personal check used to mail the funds. In no case should EEE funds released from evidence be taken up as an addition or supplement to the EEE fund maintained by the SAC for NCISRA/NCISRU operations.

g. When items have been determined to have no further evidentiary value (including possible use in appellate action) and a final authority for disposal has been obtained, they shall be removed from the evidence system. For accountability purposes, the ECD will continue to be executed until actual disposal takes place, i.e., destruction, return to command/owner, or transfer to another agency. Should an item then require shipment to another agency or, as in the case of some tape recordings, require transfer to NCISHQ for further retention, the transfer should be affected without chain of custody documents.

13-12.2. Under no circumstances will any evidence be converted for use by an NCIS component, or for the personal use of any individual within or without NCIS.

13-12.3. Should any other type of final disposal of evidence be contemplated, prior caseby- case authorization from the parent NCISFO is required. In the event it is granted, such documentation

authorizing the disposal shall be attached to the ECD retained in the Final Evidence Disposition File, and the evidence custodian shall complete the final disposition section of the ECD.

13-13. GOVERNMENT-OWNED FIREARMS EVIDENCE

13-13.1. Normally there is no confusion between firearms assigned to NCIS personnel or components and those held as evidence. There have been instances when a NCISRA has recovered and held government-owned firearms as evidence, resulting in local ordnance organizations initiating paper work to effect permanent transfer of the firearms to NCIS. To preclude NCIS from acquiring permanent custody of evidentiary firearms, the evidence custodian should ensure that any special agent submitting government-owned firearms advises the concerned command that the firearms have been transferred to NCIS custody only as evidence. No NCIS component may accept permanent transfer of such weapons to NCIS custody without prior approval of NCISHQ, nor may an NCIS component dispose of any weapons that have received permanent custody approval without the direction of NCISHQ.

13-13.2. When making final disposition on government owned firearms no longer required by NCIS as evidence, the evidence custodian should be guided by the principle that such weapons should be returned to the command from which they were stolen/seized. If the command is local to the Evidence Facility, direct transfer can occur. Otherwise, the weapon should be forwarded, not as evidence, to NCISHQ (Code 0024B1) for further transfer to military stock.

13-14. CURRENCY AND PROCEEDS OF UNLAWFUL ACTIVITY

13-14.1. Money or other property may be seized and entered into the NCIS evidence system under circumstances suggesting that the currency or property is the fruit of illegal activity or was acquired by use of the illicitly-obtained currency. When no longer required to be maintained as evidence, and upon specific authorization of the SAC, this evidence may be disposed of as follows:

a. Currency. Dispose of in the manner set out in Section 13-12.1.d above.

b. Proceeds. All evidence that cannot be returned to the command or the owner shall be turned over to the nearest Defense Reutilization and Marketing Service (DRMS)/Defense reutilization and Marketing Office (DRMO).

13-14 If seized currency or proceeds are related to illicit drug trade, the forfeiture provisions of 21 USC Section 881 may also apply. If forfeiture is an appropriate action, it should be initiated when the currency or proceeds are first seized.

13-15. LONG-TERM STORAGE OF EVIDENCE

13-15.1. Per NCIS policy certain evidence, identified below, must be retained for 50 years. In addition, the Department of Justice (DOJ) National Institutes of Justice (NIJ) highly recommends

that whenever possible samples of DNA evidence are retained for future testing as additional technologies become available. Standards published by the FBI require that a DNA sample or DNA extract used in the FBI's Combined DNA Index System (CODIS) be retained in a manner that minimizes degradation. Most field offices cannot comply with these retention requirements, due to a lack of space and adequate refrigeration facilities. To ensure the integrity of such evidence is properly maintained, a Long-Term Storage (LTS) Facility consisting of a walk-in refrigerator and a room temperature room has been constructed at Norfolk, VA.

13-15.2. LTS SUBMISSION DEFINITION AND CRITERIA

LTS evidence is evidence that must be retained for a period of time that extends beyond the expected period of time required for the trial and appeal process, i.e., 50 years. No classified material will be stored at the LTS Facility. Evidence submitted to the LTS is considered a permanent transfer. All evidence submitted to LTS must meet one or more of the following criteria:

a. Unknown (stranger) subject sexual assault kits and related evidence from unresolved rape investigation cases. Prior to submission to LTS, these kits should be submitted to an approved DNA laboratory for profiling and CODIS input.

b. Sexual assault evidence from cases in which no suspect has been identified (not indexed in NI title block) and which have been in extended retention for at least 1 year.

c. Evidence from unresolved death investigation cases that have been in extended retention for at least 1 year.

d. Evidence from significant cases as designated by NCIS HQ (DAD Criminal Investigations) that have been in extended retention for at least 1 year.

13-15.3 SUBMISSION PROCESS

All evidence being considered for transfer to LTS must be reviewed by the submitting field office's Assistant Special Agent in Charge (ASAC). The ASAC will ensure that the evidence meets the required criteria as described above. Upon receipt of ASAC approval, the following transfer process will be observed:

a. Case files ***will not*** be transferred or sent to LTS in concert with the evidence. They will be maintained as appropriate in their respective originating field office or transferred to NCISHQ.

b. Prior to packing evidence for shipment to LTS, the LTS Evidence Custodians must be contacted for specific packing requirements for multi-items of evidence.

c. The LTS Evidence Custodians must be notified of any evidence with unique storage and/or shipping requirements (i.e. furniture or other bulky items) as soon as possible prior to the transfer and shipment.

d. NCIS Form 5580/59 (12-06) will be completed by the submitting field office and must accompany all evidence submitted to LTS (refer to Appendix (1)).

e. The LTS Evidence Custodians will be notified at least 24 hours prior to shipment of the evidence.

f. Once evidence is accepted at the LTS, a copy of the completed ECD and the NCIS Form 5580/59 (12-06) will be returned to the submitting field office for placement in the case file.

13-15.4 MANAGEMENT OF THE LTS

The Special Agent in Charge, Norfolk Field Office has responsibility for organizational management of the LTS Facility, which is considered an extension of the Consolidated Evidence Facility (CEF). Only the CEF-Norfolk Evidence Custodians and the Supervisor will have access to the LTS Facility. Required LTS custody records will be kept per the requirements mandated for other evidence, as discussed previously in this Chapter. A separate Log Book will be used by the LTS Facility to document evidence transfers. A100% inventory of all LTS evidence will be required every 2 years (in contrast to the annual inventory required of other evidence storage areas).

13-15.5 TRACKING OF EVIDENCE IN THE LTS

Evidence should be disposed of once the corresponding case file is destroyed. The LTS Facility will submit an annual report to each field office SAC, listing all LTS evidence being held in conjunction with cases for which a particular field office has cognizance. (This report will include CCN, field office log numbers, and associated LTS Log numbers.) This list must be reconciled with field office records, with any resulting discrepancies being resolved in a timely manner. The LTS Facility will have blanket authorization to destroy all evidence 50 years from the date of evidence submission to the LTS Facility, unless written notification is provided to the LTS Facility requesting continued retention. The LTS Facility will formally notify the submitting field office when evidence is about to be destroyed. Evidence in LTS can be destroyed prior to the 50-year-retention date, as warranted, by authorization submitted by the case-responsible field office or NCISHQ. Prior to the actual destruction of the evidence, the LTS Evidence Custodian may verify that the case file has been or is about to be destroyed, by checking for the imaged version of the case file in the Records and Information System (RIMS) or by contacting the NCISHQ Files Section (Code 11C12) of the Records Management Branch (Code 11C1).

13-15.6 REVIEW OF EVIDENCE STORED IN THE LTS

To review LTS evidence, the LTS Evidence Custodians must be notified by the SSA involved as much in advance as possible. Efforts should be made to review the evidence in at the LTS facility in Norfolk, Virginia.

13-16 STORAGE OF ORDNANCE AS EVIDENCE

13-16.1 When arms, ammunition, and explosives are seized as items of evidence in an investigation particularly case must be employed in the storage of such items. Ammunition and explosives may deteriorate in storage. Accordingly, all DON activities shall store only arms, ammunition, and explosives for which there is a clear audit trail and an authorized reason for storage at that activity. Storage of weapons, ammunition, or explosives on an installation will be authorized by the Commanding Officer/Commanding General or a designated representative in writing. DON shore activities shall not store any ammunition and explosives that is in excess to their ammunition storage allowance. Non-government arms, ammunition, and explosives will be stored in an armory, ready service locker, or weapons magazine, but not in the same security container, weapons rack, or other storage conveyance with government arms, ammunition, and explosives. Arms/weapons will not be stored together with ammunition or explosives in the same container or safe. Arms/weapons will be stored only in a verifiable "safe" condition.

13-16.2 Explosives, ammunition, or ammunition components shall not be stored outside of approved and authorized metal containers. Arms, ammunition, or explosives will not be permanently stored in paper or plastic bags or containers. Metal containers utilized for ammunition/explosives shall be clean, dry, properly marked, and tagged (DD Form 1574) before being stored. Open containers or containers insecurely fastened shall not be allowed in authorized magazines or storage areas. If the container is unavailable, or damaged to the extent that safe storage of the contents is compromised, the contents must be transferred to a new or serviceable authorized metal container. Different types of ammunition and explosives designated by item and division may be mixed in storage provided they are compatible. Compatibility can be verified by ordnance personnel at the nearest military facility. Ammunition and explosives may not be stored together with dissimilar materials or items that present a hazard to the munitions. Examples are mixed storage of incompatible ammunition and explosives with flammable and combustible materials, acids, or solvents.

APPENDIX (1)

LONG-TERM STORAGE SUBMISSION FORM

THIS FORM AND ASSOCIATED EVIDENCE CUSTODY DOCUMENTS

MUST ACCOMPANY ALL EVIDENCE SUBMITTED TO LONG-TERM STORAGE

CASE CONTROL NUMBER (CCN): _____

SUBJECT(S):

_____

VICTIM(S):

_____

EVIDENCE LOG NUMBER(S)

LTS LOG NUMBER(S)

(EC COMPLETES LTS ONLY)

☐ SEE SEPARATE SHEET FOR ADDITIONAL EVIDENCE AND LTS LOG NUMBERS

CONTACT: PERSON WHO PREPARED EVIDENCE FOR SHIPMENTS TO LONG-TERM STORAGE:

NAME	TELEPHONE NUMBER

Based on the requirements NCIS-1 Chapter 13, 13-15.3, this evidence is authorized for long-term storage.

ASSISTANT SPECIAL AGENT IN CHARGE (TYPED NAME)	FIELD OFFICE

ASSISTANT SPECIAL AGENT IN CHARGE (SIGNATURE)

LONG-TERM STORAGE SUBMISSION FORM

CASE CONTROL NUMBER (CCN): _____

EVIDENCE LOG NUMBER(S)

LTS LOG NUMBER(S)

(EC COMPLETES LTS ONLY)

APPENDIX (2)

127772 16:09 20110726 IN:SSDEMAIL #28902 OUT:NCISHQWWSSD #249

GENERAL ADMINISTRATION 26JUL11

FROM: 0000 GEN: 11-0028

TO: DIST

SUBJ: NCIS POLICY DOCUMENT 11-16: OPERATIONAL (RETENTION OF EVIDENCE HAVING ACADEMIC OR HISTORIC SIGNIFICANCE)

1. This policy Gen Admin announces new procedures for the retention of evidence stored in the NCIS evidence custody system that is found to have academic or historic significance. The procedures described in this document create a new authorized evidence disposal method.

2. Effective immediately, evidence subject to destruction under the provisions of NCIS-3, Chapter 13 (Evidence Custody System), and determined by the Director or his designee to have academic or historic significance, may be retained by the Director or his designee for display. The Director has designated the Executive Assistant Director (EAD), Criminal Investigations Directorate (CRIM), as his designee.

3. When field personnel have identified a piece of evidence with potential academic or historic significance, an e-mail shall be sent to EAD CRIM via their chain of command. When the Director or EAD CRIM designates an item of evidence for retention and display, EAD CRIM will notify the Special Agent in Charge (SAC) of the field office holding the item of evidence via e-mail. The e-mail from EAD CRIM will confirm that an item of evidence has been designated for retention by the Director and should be transferred to NCISRA Quantico. The SAC will instruct the appropriate evidence custodian where the item is stored to transfer the designated evidence to NCISRA Quantico using authorized transfer procedures contained in NCIS-3, Chapter 13. When SAC directed, the evidence custodian releasing the item shall indicate in the "Remarks" section of the Evidence Custody Document (ECD) that the item is, "Transferred to NCISRA Quantico for final disposition and display at NCISHQ". Only items of evidence subject to disposal under the provisions of NCIS-3, Chapter 13, and that have been designated by the Director or EAD CRIM are to be transferred to NCISRA Quantico for this purpose.

4. The evidence custodian at NCISRA Quantico will notify EAD CRIM when items of evidence designated for retention and display are received. Authorized disposal procedures contained in NCIS-3, Chapter 13, will be used to release the evidence to EAD CRIM. When obtaining items for display from NCISRA Quantico, EAD CRIM shall sign the ECD to complete the final

disposition of the evidence. The signed ECD will be returned to the NCISRA Quantico evidence custody system for retention in the final evidence disposition file, per existing policy.
5. Under no other circumstances will any evidence be converted for

26JUL11

SUBJ: NCIS POLICY DOCUMENT 11-16: OPERATIONAL (RETENTION OF EVIDENCE

use by an NCIS component or for the personal use of any individual. To ensure accountability over items intended for display or academic use, EAD CRIM will ensure that the item(s) are entered into the Defense Property Accountability System (DPAS).

6. This policy will be incorporated into the next revision of NCIS-3, Chapter 13.

7. POC for this document is (b)(6) @navy.mil.

DISTRIBUTION
NCIS: ALL DEPARTMENTS AND DIRECTORATES
INFO: WWSSD

CHAPTER 14
TITLE: INTERVIEWS AND INTERROGATIONS
POC: CODE 23A
DATE: AUG 07

14-1. DISCUSSION

14-1.1. General.

An interrogation is the formal and official process of examination, by the use of questioning and persuasion, to induce a person to reveal intentionally concealed information, i.e., the truth. Interrogation is an art rather than an exact science and involves considerably more than aimless, non-directional questions. Ordinarily, it is no simple task to obtain a confession of guilt, and in many cases, considerable difficulties are also encountered in obtaining helpful information from witnesses and informants. Interrogation is a most direct attack upon the integrity of the human being, and to admit guilt under interrogation is to surrender the strong instinct of self-preservation.

14-1.2. Goals.

Interview and interrogation are essentially the same process in that both are focused toward the same end result, the securing of truthful information. Interrogation has a further specific purpose, in that it is primarily a technique for securing an admission (confession) of guilt from an individual concerning commission or participation in the commission of a crime or pertinent knowledge regarding the crime. To differentiate, an interview is the formal questioning of an individual who either has or is believed to have information of interest to the agent. Interviews are normally conducted with willing witnesses, informants, sources, etc., as differentiated from interrogations which are conducted with suspects or unwilling witnesses. In either case, the agent must control the interaction. A conversation, by contrast, implies a mutual and spontaneous exchange. An agent must master basic skills of interviewing and interrogating to be successful.

14-1.3. Approach.

There are many different effective interview/interrogation approaches and a successful approach on one individual may be totally ineffective against a twin sibling. Flexibility in technique is the key to a successful interview or interrogation.

14-2. ETHICS OF CRIMINAL INTERROGATIONS

Some of the methods discussed herein may appear in a sense, to be "unfair" to the suspect. However, none are apt to induce an innocent person to confess to a crime the person did not commit or provide information that is not the truth. Consider the narcotics dealer, the rapist, the robber or the murderer. It is naive to think an agent can hand these persons a pencil and paper and trust their conscience will impel them to confess. Unless a skillful, tactful interrogation is conducted, they may well remain undetected to commit similar or more serious crimes. Criminal interrogations will never replace thorough, professionally-conducted investigations; however, one necessarily complements or, in the best instances, corroborates the other. Each is vital to a successful resolution and a determination of the truth.

14-3. LEGAL CONSIDERATIONS FOR INTERROGATION PROCEDURES

14-3.1. Interrogation is a systematic persuasion process that is conducted by the agent in a business-like and humane atmosphere. Current legal restrictions on interrogations are based on the premises that:

a. A person will make false admissions to stop any physical or mental discomfort;

b. A suspect cannot be compelled to be a witness against himself/herself.

14-3.2. NCIS agents are charged to resolve issues and determine the truth, not to extract spurious confessions. Consequently, an agent must avoid coercion, unlawful influence, and unlawful inducement, such as promises or threats of any kind, either expressed or implied. An interrogation that is prolonged so as to deny the suspect reasonable opportunities for mental relaxation, food, drink, use of toilet facilities, etc. is prohibited. Any type of physical mistreatment or degradation is prohibited.

14-3.3. A full discussion of the legal aspects of this issue, to include custodial and non-custodial interrogations, is contained in NCIS-3, Chapter 7.

14-4. THE CONFESSION

(b)(7)(E)

Pages 395 through 419 redacted for the following reasons:
- -
(b)(7)(E)

CHAPTER 15
TITLE: PHYSICAL SURVEILLANCE
POC: CODE 22
DATE: MAR 09

APPENDICES:
(1) NCIS SURVEILLANCE DEFINITIONS
(2) NCIS 3851/1 SURVEILLANCE REQUEST/TARGET DATA WORKSHEET
(3) NCIS 3851/2 CASING REPORT
(4) NCIS 3851/3 SURVEILLANCE OPERATIONS PLAN
(5) NCIS INVESTIGATIVE ACTION – RESULTS OF SURVEILLANCE REPORT EXAMPLE
(6) NCIS 3851/4 AVIATION SUPPORT REQUEST
(7) NCIS 3851/5 AIR OPERATIONS PLAN

POLICY DOCUMENT:

APPENDIX (8): Gen Admin 11C-0004 of 7 Feb 2013 released NCIS Policy Document 13-02: Operational (Physical Surveillance Approval for National Security Investigations). Policy Document 13-02 contains revised or new policy that has not been incorporated into this chapter and should be reviewed in its entirety.

15-1. GENERAL

Surveillance is the process of keeping under observation persons, premises, or vehicles for the purpose of learning as much as possible about activities, operations and contacts for intelligence or evidentiary purposes. It is one of the most important means of protecting naval activities, securing evidence against offenders, and collecting information of both a criminal and Counterintelligence (CI) nature. Surveillance is a basic technique of present day investigative work, and is, therefore, a necessary part of the training of every investigator. It is essential for an investigator to consider employing surveillance in an investigation and/or operation because in many instances evidence and/or intelligence may not be attainable in any other way. Personnel should be familiar with the basic steps involved in planning and executing surveillance

operations. This chapter cannot, and is not designed, to cover every conceivable aspect of surveillance operations, however, it is the chapter's intent to provide a surveillant with sufficient information to plan and execute a basic surveillance operation. It would be prudent for special agents involved with counterintelligence surveillance activities to be familiar with the provisions of Executive Order (EO) 12333 (4Jan81) "United States Intelligence Activities, DoD Directive 5240.1 (25Apr8 '8) DoD Intelligence Activities, DoD 5240.1-R (11Dec82) "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons" and the Director of Central Intelligence Directive (DCID) 5/1P (19Dec84). In addition to the above listed references, it is important that surveillance personnel familiarize themselves with definitions of commonly used surveillance terms utilized throughout the U.S. Intelligence Community (IC) and Law Enforcement (LE). These definitions can be found in Appendix (1).

15-2. PURPOSES OF SURVEILLANCE

15-2.1. In investigative/intelligence work, surveillances are usually conducted for the following purposes:

a. Determine the nature and scope of suspected activities in which the NCIS has a legitimate interest and/or jurisdiction.

b. Determine the nature, degree and extent of association of a person of interest with other persons.

c. Obtain specific evidence of value for use in prosecution.

d. Locate the residence, place of employment, activity and/or contacts of individuals in whom the NCIS has a legitimate interest and/or jurisdiction.

e. Obtain other information or evidence of criminal violations.

f. Prevent a suspect from committing a crime.

g. Examine the activities of informers, informants, and military personnel who may be suspect.

h. Locate and identify undercover communication systems and courier services.

i. Exert the pressure that will cause a subject to make a mistake and expose illicit activity.

j. Determine the routes and routines followed by suspects.

k. Identify an unknown suspect or hostile intelligence officer/agent.

l. Provide safety for undercover NCIS personnel engaged in undercover operations.

15-2.2. Under DoD 5240.1-R, Chapter 9, prior approval from the Executive Assistant Director (EAD) for Counterintelligence, NCIS Code 22, NCISHQ is required before initiating a physical surveillance of United States persons for intelligence or counterintelligence purposes.

a. DoD 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons" implements DoD Directive 5240.1 and E.O. 12333 which permits physical surveillance of U.S. persons under the following circumstances:

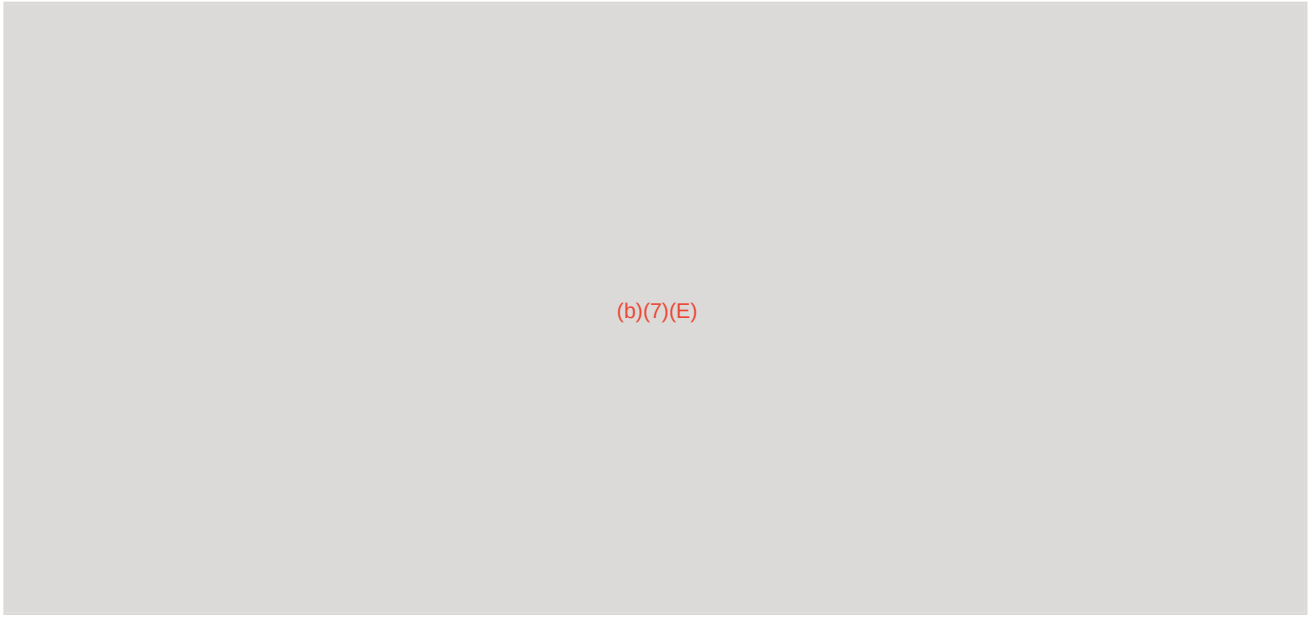
(1) Within the United States surveillance of a present or former employee of the Department of the Navy (DON), its present or former contractors or their present or former employees, applicants for employment at the DON or at a contractor of the DON for the purpose of protecting foreign intelligence or CI sources or methods or national security information from unauthorized disclosure.

(2) Outside the United States a U.S. person who is reasonably believed to be acting on behalf of a foreign power, engaging in international terrorism, narcotics activities, or activities threatening the national security of the U.S.

(3) A U.S. person, who is in contact with a person, former contractor or employee; or with a non-U.S. person who is the subject of a foreign intelligence or CI inquiry, but only to the extent necessary to identify such United States person.

b. Requests for authorization to conduct surveillance should be sent via appropriate lead tasking/notification to the appropriate NCISHQ directorate; however, under exigent circumstances, verbal approval may be authorized and subsequently followed up with appropriate documentation.

15-3. PERSONNEL CONSIDERATIONS



Pages 423 through 496 redacted for the following reasons:
- -
(b)(6), (b)(7)(C), (b)(7)(E)
(b)(7)(E)

NCIS-3, CHAPTER 16
ARREST AUTHORITY AND MILITARY APPREHENSION
EFFECTIVE DATE: MAY 2013

Table of Contents

16-1. Purpose. This chapter establishes the policy for responsibilities, requirements and standards for conducting arrests and apprehensions. Information contained in this chapter is based on the higher authorities cited in this text. The provisions of this chapter apply to all NCIS special agents who exercise arrest and apprehension authority.

16-2. Policy. NCIS personnel shall exercise arrest and apprehension authority consistent with this chapter and applicable law.

16-3. Cancellation. NCIS-3, Chapter 16 Arrest Authority and Military Apprehension, Jul 07.

16-4. Chapter Sponsor. The chapter sponsors for this chapter are the NCIS Counsel to the Director (Code 00L) and the NCIS Inspector General (Code 00I).

16-5. Definitions and References

a. Apprehension. The taking of a person into custody.

(1) Who may be apprehended? A person subject to the Uniform Code of Military Justice (UCMJ) or trial thereunder may be apprehended for an offense triable by court-martial upon probable cause to apprehend. Probable cause to apprehend exists when there are reasonable grounds to believe that an offense has been or is being committed and the person to be apprehended committed or is committing it.

(2) Who may apprehend? UCMJ Article 7, and Rule for Courts-Martial (R.C.M.) 302(b)(1), gives NCIS special agents (military and civilian) the authority to apprehend any person subject to trial by court-martial. Certain other law enforcement officials, military members, and civilians who are specifically mentioned in R.C.M 302(b) may apprehend as well.

b. Arrest. The taking of a person into custody.

(1) Who may be arrested? Military and civilian persons in violation of Federal law.

(2) Who may arrest? Within the Department of the Navy (DON), only NCIS civilian special agents have the authority to arrest persons suspected of violating Federal law.

c. Detention. A brief, temporary stop of a person as a part of an investigation for the purpose of making a limited inquiry into possible criminal activity.

d. Frisk. A limited search for weapons, generally of the outer clothing, but also of those areas which may be within a subject's immediate control.

e. Mere Suspicion. The lowest level of knowledge; nothing more than a hunch, which is not sufficient for the purpose of taking forcible action against a person.

f. Probable Cause. Information that a reasonable person would deduce that either a crime is being committed or has been committed, or that this particular person has done or is doing the crime.

g. Reasonable Suspicion. Specific and articulable facts that support a reasonable and rational inference that a crime has been, is being, or is about to be committed.

h. Seizure. The taking of a thing into possession, the manner of the taking and whether such taking is actual or constructive depending upon the nature of the thing seized.

i. 10 U.S.C. § 7480 - Authorizes the Secretary of the Navy (SECNAV) to permit civilian NCIS special agents to execute federal arrest warrants and make arrests in accordance with 10 U.S.C. § 1585a. The SECNAV exercised his authority in 2002, under 10 U.S.C. § 7480, granting arrest authority to civilian NCIS special agents, subject to the SECNAV arrest authority guidelines, which were approved by the Secretary of Defense and the Attorney General. Those guidelines are included as Appendix (A). The authority to make arrests and to apply for and execute warrants pursuant to the provisions of the guidelines is to be exercised in furtherance of the NCIS mission as specified in Secretary of the Navy Instruction 5520.3B [now SECNAVINST 5430.107, Mission and Functions of NCIS] and within the limitations of Secretary of the Navy Instruction 5820.7B [now SECNAVINST 5820.7C, Cooperation With Civilian Law Enforcement Officials]. The guidelines state that "it is NCIS policy that when the need to make an arrest is reasonably foreseeable, a warrant shall be obtained. Arrests with warrants may only be made in connection with official NCIS activities. Decisions to seek arrest warrants should be coordinated with the appropriate U.S. Attorney's Office." Additionally, these guidelines provide for limited authority to make arrests without warrants, stating: "Authority for warrantless felony arrests exists for felonies committed in the Special Agent's presence, as well

as for crimes not committed in the Special Agent's presence, if the Special Agent has probable cause to believe that the person to be arrested has committed or is committing a Federal felony and the Special Agent believes that obtaining a warrant would substantially increase the potential for escape or destruction of evidence. Authority to make warrantless misdemeanor arrests is limited to Federal crimes committed in the Special Agent's presence. Such misdemeanor arrests are discouraged." NCIS arrest authority under the guidelines applies only within the jurisdiction of the United States. NCIS arrest authority outside the United States is governed by Department of Defense Instruction 5525.11, Criminal Jurisdiction Over Civilians Employed By or Accompanying the Armed Forces Outside the United States, Certain Service Members, and Former Service Members (see subparagraph l below).

j. Federal Rules of Criminal Procedure

(1) Rule 3: The Complaint

(2) Rule 4: Arrest Warrant or Summons upon Complaint

(3) Rule 5: Initial Appearance Before the Magistrate

(4) Rule 9: Warrant or Summons upon Indictment or Information

k. Manual for Courts-Martial, United States, 2012 Edition

l. The Military Extraterritorial Jurisdiction Act. The Military Extraterritorial Jurisdiction Act (MEJA) of 2000 grants the United States District Courts jurisdiction over certain felony crimes occurring outside the United States that are committed by persons who are employed or accompanying the Armed Forces outside the United States. The Secretary of Defense, under MEJA (18 U.S.C. §§ 3261-3267), implemented by DoD Instruction 5525.11, authorized military and civilian special agents of NCIS (and other listed personnel in DoD) to make an arrest outside the United States for offenses under MEJA.

16-6. General Considerations for Arrests and Apprehensions. The single most dangerous task in law enforcement is making an arrest or apprehension. More law enforcement personnel are killed during arrests than any other phase of their work. There is no such thing as a "routine" arrest or apprehension, because there is no means available to predict how a subject will react when deprived of personal liberty. The following are prime safeguards for a successful arrest or apprehension; good judgment based upon experience and proper planning, the use of sufficient personnel who are adequately trained, and constant alertness on the part of all persons participating in the arrest or apprehension.

a. Safeguards for an Arrest or Apprehension. Always consider that the subject to be arrested or apprehended may be armed and may attempt to injure or kill the special agent if given the opportunity. When the person to be arrested or apprehended is known to be armed and dangerous or known to belong to an organization whose doctrine includes violence, extreme care and caution must be exercised. A "good" arrest or apprehension is one that results in the immediate peaceful submission of the subject to custody, and his or her subsequent safe delivery to appropriate authority.

b. Planning an Arrest or Apprehension

(b)(7)(E)

Pages 501 through 517 redacted for the following reasons:
- -
(b)(6), (b)(7)(C), (b)(7)(E)
(b)(7)(E)

CHAPTER 17
TITLE: SEARCH AND SEIZURE
POC: Code 00L
DATE: DEC 07

17-1. GENERAL

17-1.1. The Fourth Amendment, U.S. Constitution. The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the person or things to be seized.

17-1.2. The Exclusionary Rule. Evidence obtained as a result of an unlawful search or seizure is inadmissible at trial to prove the guilt of the accused. This basic concept, known as the "Exclusionary Rule" makes an understanding of the law of search and seizure essential to the proper investigation of a criminal offense. This chapter addresses the techniques to be followed to ensure that a search and/or seizure is lawful and the evidence obtained is admissible. The rules of search and seizure discussed in this chapter are not applicable to "inspections and inventories" conducted in accordance with Rule 313 of the Military Rules of Evidence.

17-2. PURPOSE AND OBJECTIVES OF A SEARCH

17-2.1. A search may be conducted by an investigator seeking many different things for a variety of purposes.

a. Evidence of a crime

b. Illegal goods

c. Government property

d. Weapons

e. Investigative leads.

17-2.2. Generally the objective of a search is dictated by the type of crime or activity being investigated. Some examples of items which may be common to various types of investigations and which may be evidence or furnish investigative leads are: computers, computer media, personal digital assistant (PDA), and cell phones letters, items of mail, notes, memoranda, address books, diaries, waste basket contents, checkbook stubs/cancelled checks, bills, luggage, claim checks, pawn tickets, maps, public conveyance schedules/tickets, newspaper clippings, notations of names or telephone numbers, matchbook covers and other advertising items, and items of clothing. These are in addition to specific items relevant to the particular investigation.

a. In National Security Investigations, the products of espionage, sabotage or subversion may include original and copies of official documents reports, descriptions, samples or models of military subject matter; communication ciphers or secret inks; maps of military areas or roads, building charts or sketches; notations and written calculations of obscure significance; plates, photographs, motion picture negatives, microfilm reels and electronic media; propaganda leaflets and other subversive literature, membership lists, organizations charts, and books and other publications that illustrate the general character of a suspect's library, if any. The tools of espionage and sabotage may include weapons; chemicals, abrasives, and explosives; drugs, narcotics, bacterial cultures, and poisons; short-wave radio equipment; computers, computer media, PDAs, cell phones; copying cameras and micrographic outfits; binoculars, telescopes, telephoto camera lenses, copying paper; key sets and burglar tools; miniature cameras; code books; supplies of inks, seals, blank passports, identification cards, credentials, and other documents; stamps, letterheads and official stationery; medicines, tablets, toilet articles or perfumes containing silver compounds, cobalt salts, potassium ferrocyanide, ammonia or other chemicals used in the manufacture or development of secret inks; articles which prevent the leaving of fingerprints, such as rubber or silk gloves, collodion and Nu-Skin; photographs and dossiers of officials or persons of military importance; and large amounts of cash or travelers' checks.

17-3. LAWFUL SEARCHES

17-3.1. The following may be seized during a lawful search.

a. Evidence of a commission of a criminal offense.

b. Contraband, the fruits of crime, or things otherwise criminally possessed.

c. Property designed or intended for use or which is or has been used as the means of committing a criminal offense.

17-3.2. The NCIS agent can anticipate participating in a variety of different types of searches during his or her career including:

a. Searches requiring probable cause (see also Military Rule of Evidence 314.).

(1) Searches conducted pursuant to a search warrant issued by competent civilian authority; and

(2) Searches conducted pursuant to an authorization to search issued by competent military authority.

b. Searches not requiring probable cause.

(1) Search incident to lawful stop

(2) Search incident to apprehension or arrest

(3) Consent search

(4) Emergency search to save life or for a related purpose

(5) Border searches; searches upon entry to or exit from U.S. installations, aircraft, and vessels abroad; searches of government property; and searches of open fields and woodlands; and

(6) Searches within jails and confinement facilities.

c. The admissibility of evidence seized will depend upon the legality of the search. Evidence seized during a search incident to apprehension, for example, is inadmissible where the apprehension is unlawful. Similarly, evidence seized during a consent search is inadmissible where the consent is later found to have been coerced or to be otherwise inadequate. Likewise, evidence seized pursuant to either a search warrant or an authorization to search is inadmissible where the warrant or authorization was issued without probable cause. Sections 17-4, 17-5 and 17-6 discuss the documents that must be prepared prior to the execution of the latter three types of searches and the minimum reporting requirements for each.

17-4. SEARCH BY WARRANT

17-4.1. Unless consent to search has been given, a valid search warrant is required before a government official can search private property located outside the confines of a military installation. The procedures to be followed to obtain a search warrant are:

a. Contact and brief the local U.S. Attorney on the facts and status of the investigation.

b. If the U.S. Attorney or Assistant U.S. Attorney determines a search is appropriate and that probable cause for issuance of a search warrant exists, the agent should prepare a search warrant and affidavit in support of the request for the search warrant. To the maximum extent possible, the agent should obtain and rely upon the advice and counsel of the U.S. Attorney.

(1) The search warrant should identify with specificity the property, person or place to be searched and identify the things to be seized.

(2) The affidavit must set forth the grounds establishing the probable cause. Accordingly, all the facts relied upon by the affiant in seeking the issuance of a warrant, including hearsay, should be

included in the affidavit. If information received from a source is included in the affidavit, the affiant must indicate why he believes the source is reliable and how the source obtained the information, if known. The affidavit should attribute all factual information to the source of that information.

(3) Once the U.S. Attorney or Assistant U.S. Attorney has approved the affidavit, the U.S. magistrate or judge should be telephonically contacted to assure that he would be available to accept and act on the affidavit.

(4) After the affidavit is executed and sworn to by the agent, the magistrate or judge, if satisfied as to probable cause, issues the search warrant. Most search warrants are issued for daytime service only; accordingly, timely execution of a search warrant is important. The law provides, however, that a search based upon a warrant for daytime service only, if initiated in daylight, can continue into darkness.

c. State and local courts and magistrates may also be used to obtain search warrants. The local prosecuting attorney, clerk of court, or local law enforcement agency should be consulted for information on the local process.

17-4.2. Upon completion of the search, the agent who secured the search warrant must leave a copy of the search warrant with the occupant of the premises or, in the occupant's absence, properly displayed on the entrance of the premises.

17-4.3. Following completion of the search, the agent who obtained the warrant must complete the reverse portion of the warrant relative to when and where he served the warrant and what he seized. The agent must then take this warrant, with the "return" portion completed, to the magistrate or judge who issued the warrant within ten days of the date of issue and complete the oath portion of the "return" in the presence of the magistrate or judge.

17-4.4. In reporting a search conducted under the authority of a search warrant, the following minimum details will be reported in the Report of Investigation (ROI) under the appropriate search caption:

a. The information utilized in the application for the warrant (a copy of the affidavit in support of the search warrant and a copy of the warrant and return should be attached to the ROI).

b. The facts surrounding the execution of the warrant.

c. A description of all items seized, including the identity of the person who has custody and the location where stored.

d. A statement that the requester of the investigation, if any, has been apprised of the results.

17-5. SEARCH BY CONSENT

17-5.1. A search consent/waiver granted by the person in possession of the property to be searched

is commonly used by NCIS agents. The lawfulness of a consent search is contingent upon obtaining the true consent of the individual solicited. Therefore, it is essential that there be an affirmative showing that the request for consent encompassed all of the legal prerequisites of true consent. This is accomplished by use of a Permissive Authorization for Search and Seizure (PASS) form (Appendix 1). The PASS form will be executed by the subject in every instance where a consent search is conducted. In those rare emergency situations where it is not feasible to reduce a consent to writing, oral consent to search must be adequately witnessed and contain all of the elements of a written consent. The ROI, entry or attachments thereto, should include:

a. The location of the original consent waiver form and a statement that copies are attached to the report.

b. The time and date the search was conducted and identification of all persons present.

c. The steps taken, if any, to ensure privacy.

d. The location where pertinent evidence was found.

e. A description of all items seized and an indication that they were properly receipted.

f. The location where the evidence is stored and a notation that the appropriate command or prosecutor is aware of its location.

17-6. SEARCH BY COMMAND AUTHORIZATION

17-6.1. The authority to search issued by competent military authority to search a person or an area, like its civilian counterpart, the search warrant, must be based upon probable cause.

17-6.2. Application for Command Authorization. The agent must provide competent military authority with the grounds necessary to enable the competent military authority to determine if probable cause exists. An application is made in writing utilizing the Affidavit for Search Authorization. The application should contain all of the rationale presented to the military authority. Based on the agent's request for authority to search, the military authority will grant or deny the request. If authority is granted, it should be reduced to writing using the "Command Authorization for Search and Seizure" format. The ROI should include, at a minimum, the following details:

a. The location of the original application for command authorization and the search authorization document and a statement that copies are attached to the report.

b. The time and date of search and identification of all persons present.

c. The steps taken to ensure privacy during search.

d. The location where pertinent evidence was found.

e. The description of all items seized and indication that they were properly receipted.

f. The location where the evidence is stored and a notation that the appropriate command is aware of its location.

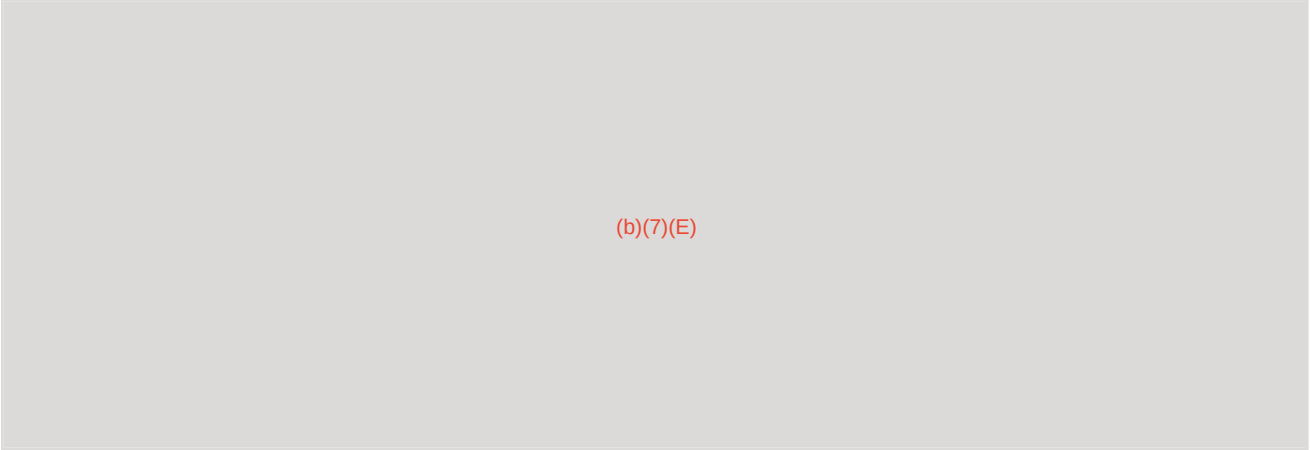
g. An indication that the competent military authority authorizing the search was apprised of the results.

17-7. SEARCH CONSIDERATIONS

17-7.1. Careful planning and preparation are essential before conducting a legal search. Depending on the type of search and specific unique situation, the agent may have only one opportunity to conduct the search and obtain evidence. If a second search can be conducted, an article or piece of evidence may have been destroyed or removed prior to the second search. The search party should be under the direct leadership of, and responsible to, one person who will serve as both coordinator and decision maker. To ensure complete coverage, assisting agents should be assigned specific tasks to perform and areas to search. Mechanical aids such as camera equipment, fingerprinting equipment, and test kits should be on the scene with persons trained in their operation available to the search party. Each agent involved in the search should be briefed as to the size and nature of the items sought, likely hiding places, and methods of recognition. Agents conducting the search should be afforded appropriate clothing and protective garments (gloves) to minimize health hazards. Provisions must be made for the proper collection, assembling, marking and preservation of the evidence seized. Adequate time must be allowed for a thorough search.

The search should proceed to its conclusion without interruption. The speed with which the search is conducted will depend upon the degree of thoroughness desired. The search should be conducted with the same degree of thoroughness throughout the entire search to avoid the necessity of repetition. Items seized should be identified and recorded, however, the agents should not conduct detailed examinations at the scene of the search. A crime scene search must be thorough and systematic (see NCIS-3, Chapter 12). It may be desirable to make a photographic and/or audio record of the search scene for future investigative assistance or as evidence. Once an item is seized as evidence it must be controlled. (See NCIS-3, Chapter 5 for discussion of items, which may legally be seized).

17-8. PRACTICAL CONSIDERATIONS WHEN CONDUCTING SEARCHES



Pages 524 through 525 redacted for the following reasons:
- -
(b)(7)(E)

APPENDIX (1) - Permissive Authorization for Search and Seizure

PERMISSIVE AUTHORIZATION FOR SEARCH AND SEIZURE

Date: _____

I, _____, after being advised by_____that the Naval Criminal Investigative Service is conducting an investigation into _____ _____, have been requested to permit a search of my_____ _____.

I have been informed of my constitutional right to refuse to permit this search in the absence of a search warrant. In full understanding of this right, I have nevertheless decided to permit this search to be made.

This search may be conducted on _____ by_____and I hereby give My permission to remove and retain any property or papers found during the search which are desired for investigative purposes.

I make this decision freely and voluntarily, and it is made with no threats having been made or promises extended to me.

Signed: _____

_____
Representative, Naval Criminal Investigative Service

_____
Representative, Naval Criminal Investigative Service

_____
Command Representative

TIMES OF SEARCH

Start: _____ _____

End: _____ _____

CHAPTER 18
TITLE: POLYGRAPH
POC: CODE 24B2
DATE: AUG 07

18-1. NCIS POLYGRAPH PROGRAM. The polygraph is a credibility assessment process dating back to the 1920's. NCIS incorporated its use in 1948 and the polygraph's modern form is best described as an examination utilizing Polygraph and Credibility Assessment (PCA) techniques to determine an individual's truthfulness/credibility. While NCIS recognizes the polygraph as an invaluable investigative aid, it should never be considered a substitute for conventional investigative techniques.

18-2. DIRECTIVES AND POLICY.

18-2.1. Department of Defense (DOD) Directive 5210.48, Department of Defense Polygraph Program, sets forth conditions within the Department of the Navy (DON) under which polygraph examinations may be conducted, as well as the requirements for selection, training, and supervision of polygraph examiners. This instruction specifically delegates the authority to approve polygraph examinations within the DON to the Director, NCIS or his/her designee. It also identifies the Director as the sole authority within the DON for certifying which examiners are qualified and competent to conduct polygraph examinations. Within the NCIS, the Director has designated the Chief of the Polygraph Services Division (Code 24B2) as having exclusive responsibility for both approving polygraph examinations and making final recommendations for certifying or decertifying polygraph examiners.

18-2.2. The Federal Polygraph Examiner Handbook (CIFA Technical Manual, 09/12/05) provides a reference for polygraph standards, as taught by the Defense Academy for Credibility Assessment (DACA), (formerly known as the Department of Defense Polygraph Institute - DODPI). The Handbook prescribes uniform polygraph procedures for all DOD elements and Federal law enforcement, counterintelligence, and security agencies that use PCA techniques. NCIS conducts all polygraph examinations in compliance with these standards and procedures and as specifically implemented by supplementary instructions contained in the NCIS Polygraph Program Operations Manual.

18-3. PROGRAM ADMINISTRATION.

18-3.1. Chief, Polygraph Services Division (Code 24B2). Chief, Polygraph Services Division is the senior manager of the NCIS Polygraph Program and is specifically responsible for the following:

a. Final approval authority for all polygraph examination requests within the DON.

b. Final quality control of all polygraph examinations conducted under NCIS jurisdiction.

c. Overall supervision of polygraph examiners, particularly as it pertains to:

(1) Selection, training, and probationary periods of potential examiners;

(2) Certifying and decertifying of examiners;

(3) Ensuring examiners maintain minimum technical skills;

(4) Requisite biennial refresher training of examiners; and

(5) Endorsements on all examiners' annual performance reviews.

d. Purchasing and maintaining all polygraph related equipment and supplies.

e. Operational travel funding (via the Field Services Support Department).

f. Training funding (via the Training Department).

g. Provide input and recommendations in response to Joint Staff requests for augmentation/forces of NCIS polygraph examiners.

18-3.2. Deputy Chief, Polygraph Services Division (Code 24B2). Deputy Chief, Polygraph Services Division directly assists the Polygraph Services Division Chief with the responsibilities listed above. In the absence of the Chief, the Deputy Chief is specifically delegated the authority to independently perform all duties.

18-3.3. Polygraph Supervisory Special Agents (SSAs). Polygraph SSAs act as direct representatives of the Polygraph Services Division Chief, providing critical interface between their respective Field Offices and Code 24B2 on all polygraph technical and operational matters. Polygraph SSAs are also the first-line supervisors of all examiners within their respective regions and primarily responsible for the overall quality of polygraph examinations, corrective training as appropriate, and the evaluation and documentation of technical skills in performance reviews. Polygraph SSAs may routinely grant provisional approval (preceding Code 24B2's final authorization) to conduct polygraph examinations relating to drug urinalysis tests. Otherwise, provisional approval may only be granted for polygraphs in connection with other types of cases in exigent circumstances when timeliness is critical and telephone contact with Code 24B2 is not possible. Regardless of the circumstances, the control office must submit an

official request (Section 18-5.) to Code 24B2 as soon as possible.

18-3.4. NCIS Polygraph Examiners.

a. NCIS Polygraph Examiners are either Special Agents or Security Specialists who have successfully completed the core curriculum (PCA Course) at DACA, satisfactorily served a probationary period of 6-12 months, and have been officially certified by the Director to conduct polygraph examinations. Security Specialist examiners are generally limited to conducting polygraph examinations in support of programs requiring Test for Espionage and Sabotage/Counterintelligence Scope Polygraph (TES/CSP) testing. Special Agent examiners are authorized to conduct the full range of polygraph examinations pertaining to criminal/intelligence investigations and counterintelligence/terrorism operations, as well as polygraph exams in support of programs requiring TES/CSP testing.

b. Every NCIS examiner, however, may be consulted with on the technical aspects of any type of polygraph examination, particularly with regard to the appropriateness and utility of polygraph testing for resolving issues. Examiners should not review or be asked to review ongoing cases solely for the purpose of deciding whether to offer a polygraph examination, as it is the responsibility of the SSA of the concerned field office NCISRA to make the determination. Examiners are also normally restricted from taking part in pre-polygraph interrogations to preclude any potential bias concerning an examinee's truthfulness. Conversely, with the concurrence of Code 24B2, Special Agent examiners may assist fellow agents with non-polygraph duties (i.e., protective service operations, surveillances, training, briefings, etc.) when additional manpower is needed to meet extraordinary workloads of host field offices.

18-3.5. Special Agent In Charge (SAC). SAC of a host field office provides administrative support to NCIS polygraph examiners assigned to their respective AOR. Such support includes, but is not limited to: providing appropriate office spaces, telephone and utility services, vehicles, C&CI funds, expendable supplies, minor repairs, in-service training, preparation of travel orders, and clerical support at designate locations.

18-4. REQUIREMENTS FOR POLYGRAPH AUTHORIZATION.

18-4.1. General Guidance. While polygraph examinations can be unique, decisive investigative assistance tools, the use of polygraphs are not to be used prematurely or in lieu of other available courses of action. Contrary to popular misconceptions, the polygraph technique is not an effective means for screening large numbers of potential suspects (commonly categorized as "witch hunting"), nor is it capable of establishing the intent of the individual tested. Further, polygraph examinations should not be administered immediately following a strong or lengthy confrontation with a potential examinee, as there is compelling psychological evidence indicating that such timing may adversely affect the validity of the test results. This prohibition is bolstered by DOD Regulation 5210.48-R, Department of Defense Polygraph Program, which states, "The person being considered for a polygraph examination shall be given timely notification of the date, time, and place of the examination..." Otherwise, aggressive and frequent use of polygraph is strongly encouraged and should be considered as an essential investigative step in the following described situations.

18-4.2. Investigations (Case Categories 1 Through 8). Requests for polygraph examinations will be approved if the three following criteria are met:

a. The alleged crime is an offense punishable under Federal Law, the United States Code, or the Uniform Code of Military Justice, by death or confinement for a term of one year or more,

b. The investigation has been as thorough as possible, consistent with the circumstances of the case, and the development of additional information by means of a polygraph examination would help in resolving individual culpability, and

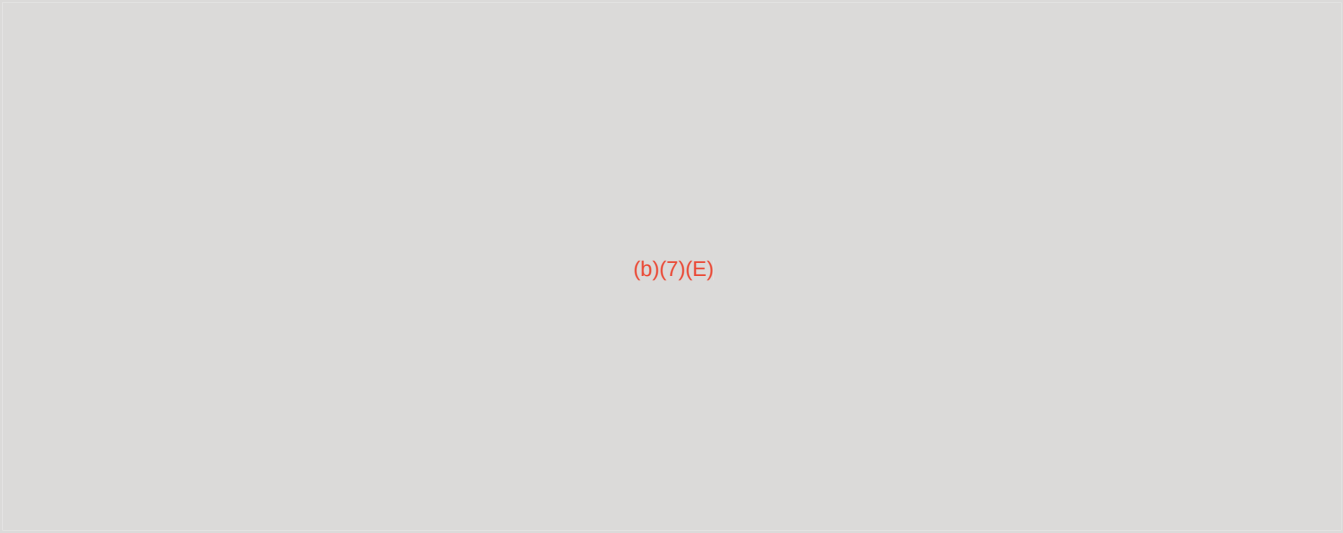
c. There is reasonable cause to believe the person to be examined has direct knowledge of or was personally involved in the matter under investigation, and is considered a:

(1) SUSPECT, and has been thoroughly interrogated with an appropriate legal warning prior to being offered an opportunity to undergo a polygraph examination;

(2) VICTIM, and there is adequate information to doubt one's veracity, and not merely because lesser rank or grade than the suspect(s) is reflected. The victim must have been thoroughly interrogated with an appropriate legal warning (i.e., false complaint, false official statement, false swearing, etc.) prior to being offered an opportunity to undergo a polygraph examination. If the investigation is predicated essentially by a victim-suspect confrontation that cannot be clearly resolved through traditional investigative means, then the suspect will be administered a polygraph examination prior to the victim. If the ensuing investigation shows obvious and substantial reason to question the victim's truthfulness, then a polygraph examination of the victim prior to the suspect may be requested. Polygraph examinations of rape victims are generally discouraged and will only be considered by Code 24B2 on a limited basis.

(3) WITNESS, and information regarding is unconfirmed or dubious and cannot be verified by conventional investigative techniques, or when timely corroboration of their information would prevent unnecessary expenditures of significant manpower or monetary costs. Otherwise, a polygraph examination of a witness may only be requested if there is substantial reason to doubt one's credibility and a thorough interrogation with an appropriate legal warning was conducted prior to being offered an opportunity to undergo a polygraph examination.

(b)(7)(E)



18-4.5. Exculpation.

a. Polygraph examinations requested may be authorized when requested by the subject of an official DOD administrative, criminal, counterintelligence, or personal security investigation to exculpate one from allegations or evidence arising in the course of such investigation. The utilization of polygraph is considered essential to a just and equitable resolution of the specific matter under investigation. Such requests must originate from the subject or representing legal counsel, and be completely free from influence or coercion (expressed or implied) from command. In all situations, prior to the administering of a polygraph examination, the subject must have undergone an interrogation with an appropriate legal warning to precisely ascertain the basis of any denials, and thereby ensuring an agreeable resolution as a result of polygraph testing.

b. If during the course of an investigation the subject has already denied specific allegations while under an advisement of rights, a re-interrogation is not necessary prior to forwarding a request for an exculpatory polygraph exam to Code 24B2. Otherwise, the responsible NCIS office must interrogate the subject before the submittal of a request to Code 24B2 for consideration. The latter applies even to pre-trial and post-trial requests emanating from the individual's defense counsel, and must be made in writing and contain an endorsement of one of the following: Staff Judge Advocate, court-martial Convening Authority, appointed Trial Counsel, Senior Trial Counsel, Appellate Government Counsel, or Special Assistant to the U.S. Attorney. The request must be forwarded to Code 24B2 for consideration, even if an endorsing authority provides a negative endorsement. The results of such examinations will be reported to both the defense counsel, as well as the appropriate endorsing authority and/or command.

18-4.6. TES/CSP Examinations (Case Category 9P). The principal purpose of a Test for Espionage and Sabotage (TES) polygraph examination, also known as a Counterintelligence Scope Polygraph (CSP), is to assist adjudicative authorities in determining the initial eligibility, and periodically thereafter on a random basis, the continued eligibility of designated personnel for access to certain classified information or positions specified by current DOD guidelines. Requests for TES/CSP examinations are generally submitted by pertinent adjudicative

authorities or commands directly to the nearest servicing NCIS polygraph examiner(s) without involving host FO personnel. All requests for TES/CSP examinations of NCIS employees or contractors and any requests from outside NCIS submitted to the host FO should be referred directly to the servicing NCIS polygraph examiner(s) for consideration. A TES/CSP examination is not technically suitable for and may not be used to resolve allegations of wrongdoing or suspicious behavior. A separate investigation should be conducted regarding such particular concerns and if subsequently deemed appropriate (per Section 18-4.1. and 18-4.2. above), a specific-issue polygraph examination may be requested.

18-5. POLYGRAPH REQUEST AND APPROVAL PROCEDURES.

18-5.1. Requests.

a. The decision to use a polygraph during an investigation is the prerogative of the SSA of the NCISRA concerned. The SSA must ensure requirements set forth in Section 18-4 are fully satisfied before permitting a control agent to offer an individual (e.g., suspect, victim, witness, CW) the opportunity to undergo a polygraph examination. When doing so, control agents should not attempt to explain polygraph procedures or the exact phraseology of questions that will be asked during the test. All queries should be answered with a general explanation such as, "The polygraph test will confirm whether you are telling the truth about (the matter under investigation). Although I'm not qualified to answer technical questions concerning polygraph, I can assure you the examiner will provide an in-depth explanation of the entire process, as well as answer every question you have before you actually take the test."

b. If a problematic situation arises when asking an individual to undergo an examination, the servicing polygraph examiner or Code 24B2 may be contacted for guidance or assistance in directly answering the potential examinee's questions. Once an individual verbally agrees to undergo polygraph testing, the control agent must submit a request to Code 24B2 to administer the examination. In urgent situations, a telephone request for authorization will be considered after all requested documentation has been faxed to Code 24B2 or reviewed by the servicing examiner. Regardless, the control office is required to submit an official request to Code 24B2 as soon as possible.

c. An investigation with a limited number of suspects will be considered for multiple authorizations requests by Code 24B2, provided the use of polygraph does not appear to be screening (see Section 18-4.1. above). If approved, the "prime suspect" will be tested first. Otherwise, the examinations will be administered in a logical sequence as determined by the servicing examiner and based on available case facts. If after agreeing to undergo a polygraph an individual terminates the interrogation or requests a lawyer, the control agent must re-contact the individual or designated defense counsel to confirm their continued willingness to undergo an examination before submitting a request for authorization to Code 24B2. All requests for polygraph authorization will be transmitted via an ROI (ACTION) with lead tasking to Code 24B2, and also listing the servicing polygraph examiner, control office, field office, and NCISHQ Directorate in the DISTRIBUTION for advance planning purposes (if the examinee is a juvenile, see Section 18-7.3. If the request relates to CI/CT operations, see: Section 18-4.4.).

EXAMPLE: ACTION
R. 0024B2: Request approval to administer a polygraph examination to S/JONES.

DISTRIBUTION
NCISHQ: 0021 (or, 0022, 0023)
ACTION: 0024B2
INFO: DCWA/DCVH

d. Strict adherence to the stated guidelines and specified rules expedites the processing of requests for polygraph examinations by Code 24B2.

18-5.2. NCIS Investigation (OPEN).

a. If the individual to be polygraphed is identified in the CASE TITLE block of the investigation, and the control office has already entered into CIS the ROIs and IAs documenting all investigative effort to date, then the NARRATIVE of the requesting ROI (ACTION) may be synoptic.

b. If the individual to be polygraphed is identified in the CASE TITLE block of the investigation, but the control office has not yet transmitted all pertinent documentation, (particularly the statements and results of interview of victims, suspects, and witnesses), then the requesting ROI (ACTION) must contain a substantial NARRATIVE explaining the investigative chronology and details leading to the need for a polygraph. The control agent must fax all the aforementioned pertinent statements and results of interviews to Code 24B2 for review.

c. If the individual to be polygraphed is not identified in the CASE TITLE block of the investigation, then he/she must be clearly identified (minimum of full name, rank, SSN, DOB, and POB) in the NARRATIVE of the requesting ROI (ACTION). Applicable rule(s) from Section 18-5.1. should be followed.

18-5.3. NCIS Investigation (CLOSED). If use of polygraph is deemed appropriate after an investigation has been closed, the control office must reopen (ROPEN) the case (see NCIS-1, Chapter 25, Report Writing) before submitting the request to Code 24B2 for final approval. Further, all requirements and procedures for requesting polygraph support remain the same as for any OPEN investigation (see Sections 18-5.1. and 18-5.2.).

18-5.4. Non-NCIS Investigations. With the concurrence of Code 24B2, NCIS examiners may administer polygraphs to assist military commanders and other law enforcement agencies with their respective investigations so long as each request meets the minimum criteria set forth in Section 18-4. Code 24B2 is empowered to authorize any request wherein the prospective examinee is a DOD employee (including those in connection with a criminal investigation conducted by a non-DOD law enforcement entity) or is a non-DOD person subject to the Uniform Code of Military Justice. Otherwise, Code 24B2 may need to obtain specific approval from the Assistant Secretary of Defense before authority can be granted to administer an exam. All polygraph requests from non-NCIS agencies must be submitted in writing with sufficient

details assuring full compliance with all aspects of current regulations. At a minimum, requests must contain all investigative reports generated to date by the non-NCIS agency. The servicing NCISRA must consequently OPEN an investigation utilizing its own CCN (i.e.; 6TNA if the police department aboard a Navy base is requesting polygraph assistance on a felony personal larceny case), and then officially request polygraph authorization by ROI (ACTION) as set forth above in Sections 18-5.1. and 18-5.2.

18-5.5. Authorizations.

a. Should all required criteria for approval not be completely satisfied, Code 24B2 will apprise the requesting control office via ROI (ACTION) of the specific reason(s) for holding the authorization in abeyance or denying the request. Otherwise, Code 24B2 will assign a unique approval number and transmit the polygraph authorization via an ROI (ACTION) with lead tasking to the servicing polygraph examiner and the control office, and with the field office and NCISHQ Directorate listed in the DISTRIBUTION for apprising purposes:

EXAMPLE: ACTION
R. DCVH: Administer a polygraph examination to S/JONES. approval number is 2004-0123.DCAN: Coordinate with DCVH to schedule the polygraph examination of S/JONES.

DISTRIBUTION
NCISHQ: 0021 (or, 0022, 0023)
ACTION: DCVH/DCAN
INFO: DCWA

b. Upon receipt of Code 24B2's approval, the control agent must coordinate directly with the servicing examiner for scheduling of the polygraph examination (Section 18-6.).

18-6. SCHEDULING AND REPORTING RESPONSIBILITIES.

18-6.1. Control Agent. Because a polygraph examination is only one of many investigative steps associated with a case, the control agent remains the party logical for ensuring that the process is satisfactorily completed. While lead tasking is sent to the servicing polygraph examiner (principally for report writing purposes), the control agent is nonetheless responsible for:

a. Coordinating with both the servicing polygraph examiner and the prospective examinee to schedule a mutually agreeable date, time, and location for the examination (Note: A minimum of 4 hours is required and it is strongly recommended that the examinee not have commitments planned within an 8-hour timeframe at the start of testing.)

b. Arranging for the use of an appropriate room to conduct the examination if an office permanently occupied by the servicing examiner is not available. Designated interview rooms are generally most desirable, but other quiet spaces (e.g., conference rooms, private offices, hotel

or BOQ rooms) are acceptable as long as access can be totally controlled by the examiner.

c. Ensuring the potential examinee commits to the agreed scheduled appointment. The examinee should not bring any other parties to the scheduled polygraph examination other than official legal counsel.

d. Being physically present and readily available to the examiner for possible consultation during the entire polygraph examination.

18-6.2. Polygraph Examiner Responsibilities. The servicing examiner will coordinate directly with the control agent to ensure the polygraph examination is completed as expeditiously as possible following receipt of Code 24B2's authorization. At a minimum the examiner will:

a. Thoroughly review and discuss the case facts with the control agent in advance of the scheduled examination to ensure the comprehensive coverage of all relevant areas during the test.

b. Assist the control agent as much as practical with selecting and preparing the room to be used for the examination.

c. Administer the polygraph examination and submit the completed polygraph package to Code 24B2 for final quality control review.

d. Finalize all statements or results of interview, documenting any new information provided by the examinee during the examination, and when possible assist the control agent with post-test collection of any evidence developed as the result of the test.

e. Prepare and transmit/ProComm (in accordance with NCIS-1, Chapter 25, Report Writing) an Investigative Action (IA) documenting the details of the entire polygraph examination, as well as an ROI (INTERIM) or ROI (ACTION) reporting the completion of the lead tasking sent by Code 24B2.

18-7. MISCELLANEOUS.

18-7.1. Declinations.

a. DOD Directive 5210.48, DOD Polygraph Program, states, "Adverse action shall not be taken against a person for refusal to take a polygraph examination in criminal or unauthorized disclosure cases. A refusal to consent to a polygraph examination shall not be recorded in the person's personnel file or any investigative file, nor shall a person's supervisor, and in the case of a contractor employee, the person's employer, be informed of the refusal unless such actions are necessary in support of action to be taken under the provisions of TES/CSP testing [Section 18-4.6.]. Refusal to take a polygraph examination shall be given full privacy protection provided for in DOD Directive 5400.11 (Department of Defense Privacy Program)." Meaning, with the exception of internal reporting to account for polygraph requests and authorizations (Sections 18-7.1.b. and 18-7.1.c. below), an individual's refusal to undergo a polygraph examination shall

not be verbally briefed to anyone outside of NCIS nor explicitly mentioned anywhere in IAs or ROIs. Substituting an alternate term for the words "Polygraph Examination" in a report is considered a transparent attempt to disguise an individual's refusal to consent to a polygraph examination. In an effort for total compliance with the intent of the regulation, the use of other terms such as "technical investigative aid" is prohibited.

b. In order to accurately document all investigative efforts and provide subsequent reviewers a clear understanding that all available forensic techniques were considered during the course of a particular investigation, the following should be written in NARRATIVE or text portions of reports:

- On ddmmyy, an attempt was made to re-interview S/JONES about his/her previous denial of culpability in (the crime). However, S/JONES exercised his/her right to remain silent by refusing to discuss this matter further.
- On ddmmyy, subsequent to waiving his/her rights, Enclosure (x), S/JONES continued to deny culpability in (the crime), and eventually terminated the re-interview by requesting to speak with legal counsel.

c. To ensure the following reports are not disseminated outside of NCIS, authors will transmit them electronically whenever possible, choosing "NO" in the "Is Document Releasable?" entry block on the "Header" window of the *SSD* Template in the NCIS Report Writing program.

(1) If an individual declines to undergo the offered polygraph after the control office has already submitted a request to Code 24B2 but has not yet been approved, the control office will send an ROI (ACTION) to Code 24B2 canceling the request:

Example: ACTION
R. 0024B2: S/JONES has declined the opportunity to undergo a polygraph. Cancel the request sent by reference (A).

DISTRIBUTION
NCISHQ: 0021 (or, 0022, 0023)
ACTION: 0024B2
INFO: DCWA/DCVH

(2) If an individual declines to undergo a polygraph examination that has already been approved by Code 24B2, the servicing examiner will send an ROI (ACTION) reporting the cancellation of lead tasking:

Example: ACTION
R. 0024B2: S/JONES has declined to undergo the polygraph authorized by reference (A), and lead tasking is therefore completed.

DISTRIBUTION

NCISHQ: 0021 (or, 0022, 0023)
ACTION: 0024B2
INFO: DCWA/DCAN

18-7.2. Prohibition Against Non-Federal Polygraphs. DOD Directive 5210.48 of 25 January 2007 stipulates that only PCA examinations conducted by Federal PCA examiners shall be accepted by DOD components.. Accordingly, when a non-NCIS or non-Federal Polygraph Examiner has administered a polygraph examination, NCIS policy mandates that a separate examination before making any statement regarding the truthfulness of the examinee be administered. NCIS examiners are precluded from reviewing an outside examiner's charts and rendering an opinion concerning their validity unless specifically requested to do so by JAG or a military judge as an expert witness providing testimonial evidence.

18-7.3. Juveniles. Written parental or legal guardian consent is required prior to submitting a request for polygraph authorization of a juvenile (See Appendix 1 for the NCIS Statement of Consent for the Polygraph of a Juvenile form). Matters in which parents or guardians are considered to be suspects because of allegations by the juvenile should be referred to Code 24B2 or pertinent prosecuting authority for guidance, as it may be impractical to obtain consent. Otherwise, a copy of the consent form must be forwarded to Code 24B2 with the request (Section 18-5.) for authorization, with the original consent form being provided by the control agent to the servicing examiner for inclusion in the polygraph package prepared by the examiner upon completion of the polygraph examination.

APPENDIX 1

NAVAL CRIMINAL INVESTIGATIVE SERVICE

STATEMENT OF CONSENT FOR THE POLYGRAPH OF A JUVENILE

_____

_____
(Location)

I, _____, being the parent/legal guardian
(Name of Parent/Guardian)

of _____ do hereby permit him/her to undergo
(Name of Examinee)

polygraph examination. The examination will be conducted pursuant to an

investigation regarding _____. I fully
(Focus of Investigation)

understand this consent is voluntary and can be withdrawn at any time. I also

understand that _____ must voluntarily
(Name of Examinee)

consent to the examination and his/her consent may be withdrawn at any time.

_____
(Signature of Parent/Legal Guardian) (Date)

_____

_____
(Address)

_____
(City, State, Zip Code)

_____
(Telephone Number)

CCN: _____

NCIS-3, CHAPTER 19
COUNTERINTELLIGENCE SUPPORT TO THE DEFENSE CRITICAL INFRASTRUCTURE PROGRAM CASE CATEGORY: XXCP
EFFECTIVE DATE: DECEMBER 2014

Table of Contents **PAGE**

References:

(a) DoD Directive 3020.40, DoD Policy and Responsibilities for Critical Infrastructure, 14 January 2010 (Incorporating Change 2, September 21, 2012)
(b) SECNAV Instruction 3501.1C, Department of the Navy Critical Infrastructure Protection Program, 13 December 2011
(c) DoD Instruction 5240.19, Counterintelligence Support to the Defense Critical Infrastructure Program (DCIP), 31 January 2014
(d) NCIS-3, Chapter 43, CI Support to Research, Development, and Acquisition, August 2013
(e) NCIS-1, Chapter 25, SSD Report Writing, January 2010
(f) DoD Manual 3020.45, Vol. 1, Defense Critical Infrastructure Program (DCIP): DoD Mission-Based Critical Asset Identification Process (CAIP), 24 October 2008

19-1. Purpose

a. The Defense Critical Infrastructure Program (DCIP) is a comprehensive program designed to protect Federal and defense critical infrastructure (DCI) and ensure the uninterrupted conduct of essential national functions. This program and the roles and responsibilities of Department of Defense (DoD) organizations are delineated in reference (a). Prioritization of assets requiring enhanced protection is categorized into the areas of defense infrastructure sectors under the direction of their Defense Infrastructure Sector Lead Agent (DISLA), defense critical assets (DCAs), and Tier 1 task critical asset (TCA).

b. The purpose of this chapter is to provide guidance on the Naval Criminal Investigative Service (NCIS) responsibility to provide counterintelligence (CI) support to the DCIP. Policy contained in this chapter enumerates requirements mandated by DoD and Department of the Navy (DON) instructions as to what support NCIS is to provide to DON critical assets and assigned DoD sectors. NCIS support of DCIP involves both the National Security Directorate (NSD) and the Directorate of Intelligence and Information Sharing (DIIS). Overall programmatic responsibility resides with NSD.

19-2. Policy. NCIS field offices will provide full-spectrum CI support to their assigned DISLAs, DCAs, and Tier 1 TCAs with operational oversight provided by the geographic executive assistant directors (EADs) and program management oversight from the NSD. The DIIS will support the field operational efforts with the production of DISLA-, DCA-, and Tier 1 TCA-specific threat assessment products. All CI support provided by NCIS field elements will be documented under the XXCP case category.

19-3. Cancellation. NCIS-3, Chapter 19, dated August 2013.

19-4. Chapter Sponsor. NSD Cyber Department (Code 22D).

19-5. General Information

a. Reference (a) defines DISLA as a designated DoD official and their respective defense sector organizations that perform defense infrastructure sector responsibilities. DISLAs characterize their defense infrastructure sectors to identify functions, systems, and interdependencies that support combatant command, military department, and defense agency missions and sector functions.

b. Reference (a) defines DCAs as being of such extraordinary importance to DoD operations in peace, crisis, and war, that their incapacitation or destruction would have a serious, debilitating effect on the ability of the DoD to fulfill its mission. DISLAs and DCAs are nominated by the Chairman of the Joint Chiefs of Staff (CJCS) and approved by the Office of the Assistant Secretary of Defense for Homeland Defense and America's Security Affairs (OASD/HD&ASA). The CJCS validates DCA locations on a yearly basis. NCIS, in partnership with the Office of Naval Intelligence and the Office of the Under Secretary of the Navy, Assistant for Special Programs and Intelligence, coordinates with the DON critical infrastructure assurance officer in developing a comprehensive indications and warning capability to identify and report on unconventional threats to the DCI, i.e. foreign intelligence services and terrorism, in accordance with reference (b).

c. Reference (a) defines a TCA as an asset that is of such extraordinary importance that its incapacitation or destruction would have a serious, debilitating effect on the ability of one or more DoD components or DISLA organizations to execute the task or mission-essential task it supports. TCAs are used to identify DCAs.

d. Reference (c) assigns DoD CI organizations lead agency responsibilities for specific defense sectors and DISLAs. The role of NCIS within the DCIP is to develop indications and warnings of threats to its assigned DISLAs, DCAs, and Tier 1 TCAs upon which appropriate actions to neutralize or exploit those threats may be taken. These threats emanate from both the physical and cyber domains and include threats from criminal elements, domestic and foreign terrorists, and foreign intelligence services.

19-6. NCIS Counterintelligence Support to DCIP

Pages 541 through 549 redacted for the following reasons:
- -
(b)(7)(E)

NCIS-3, CHAPTER 20
NATIONAL SECURITY INVESTIGATIONS
EFFECTIVE DATE: July 2014

TABLE OF CONTENTS: **PAGE**

20-1. Purpose. In 2011, the Naval Criminal Investigative Service (NCIS) Headquarters combined the Counterintelligence and Combating Terrorism Directorates into the National

Security Directorate (NSD) in order to better align resources, capabilities, and authorities. This chapter establishes policy relating to responsibilities, requirements, and standards for the conduct and management of national security investigations (NSI) as set for in references (a) - (d) and defined by reference (e) in which the initial allegation or eventual determination involves indicators of espionage, terrorism, illegal technology transfer, foreign influence, or suspicious collection activities. All references are located in Appendix A.

20-2. Policy

a. It is NCIS policy that NSIs will be conducted following the guidance set forth in this chapter and in accordance with the cited references. Reference (e) defines counterintelligence investigations as "formal investigative activities undertaken to determine whether a particular person is acting for or on behalf of, or an event is related to, a foreign power engaged in spying or committing espionage, sabotage, treason, sedition, subversion, assassinations, or international terrorist activities and to determine actions required to neutralize such acts."

(1) Reference (e) states that CI investigations of active and reserve military personnel, DoD civilians, and other DoD-affiliated personnel shall be conducted by the Military Department CI organizations (MDCO) designated by the Service Secretary.

(2) In reference (f), the Secretary of the Navy assigned the responsibility for conducting counterintelligence investigations for the Department of the Navy (DON) to the Director, NCIS.

b. The below definitions apply to this chapter.

(1) Reference (g) defines foreign intelligence entities (FIE) as "Any known or suspected foreign organization, person, or group (public, private, or governmental) that conducts intelligence activities to acquire U.S. information, block or impair U.S. intelligence collection, influence U.S. policy, or disrupt U.S. systems and programs. This term includes a foreign intelligence and security service and international terrorist organizations."

(2) A DoD-affiliated person is defined in reference (h) as "DoD active and reserve personnel, DoD civilian employees, retired military and DoD civilian personnel, contractors and their employees, inactive reservists, National Guard members, family members of active duty and civilian personnel, persons residing on or having access to DoD facilities, persons under consideration for DoD employment, and former DoD employees or contractors."

(3) Reference (a) 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 including personnel, physical, document communications security programs."

(a) CI has both an offensive mission (neutralizing or exploiting the FIE targeting national defense information, infrastructure, and assets) and a defensive mission (protecting the nation's secrets and DON assets against FIE including terrorists).

(b) Reference (b) states "Defensive CI activities shall be undertaken as part of an integrated DoD and national effort to detect, identify, assess, exploit, penetrate, degrade, and counter or neutralize intelligence collection efforts, other intelligence activities, sabotage, espionage, sedition, subversion, assassination, and terrorist activities as directed against the DoD, its personnel, information, material, facilities, and activities, or against U.S. national security."

20-3. Cancellation

a. This chapter cancels NCIS 3, Chapter 20, Espionage dated August 2007 and NCIS 3 Chapter 23, Security Matters dated December 2006, in their entirety.

b. Sections 22-1 through 22-4 of NCIS 3, Chapter 22, Internal Security Investigations, dated December 2006 are cancelled and sections 38-2 through 38-5 of NCIS 3, Chapter 38, Combating Terrorism Investigations and Operations, dated November 2008, are cancelled.

c. This chapter incorporates NCIS GEN 22-0026 dated May 3, 2013, National Security Program Guidance: Eguardian And Suspicious Incident Reporting Requirements, and that Gen Admin is now cancelled.

20-4. Chapter Sponsor. NCISHQ NSD Investigations (Code 22B) sponsors this chapter.

20-5. Objective. The NCIS is committed to operational excellence. Responsibility for the quality of counterintelligence and combating terrorism investigations is vested in that case agent and at all levels of leadership and management. The objective of this chapter is to provide guidance on the conduct, reporting, oversight, and management requirements of NSI's with the goals of:

a. Protecting DoD and DON national defense information, critical technology, infrastructure, and personnel;

b. Preserving the potential for prosecution of all culpable parties identified;

c. Contributing to the identification and elimination of security vulnerabilities;

d. Identifying information in support of existing counterintelligence collection requirements;

e. Assisting decision makers in risk management and damage assessment decisions.

20-6. General Information

Page 553 redacted for the following reason:
- - - - - - - - - - - - - - - - - - - -
(b)(7)(E)

b. Coordination. NSIs may be conducted jointly with other investigative agencies and as such, require coordination at the headquarters and field levels. In the absence of exigent circumstances such as the imminent attack on a DoD/DON installation, loss of sensitive classified material, or the possible flight of the suspect, no investigative action which would alert the suspect(s) or disclose NCIS interest in the suspect(s) should be taken until an investigative plan has been carefully considered and notification, if required, made to other agencies. NSD desk officers and attorneys should be consulted early in the development of these investigations in order to provide guidance and assistance in the coordination and use of investigative tools as well as reporting requirements. Additionally, coordination between NSD investigations and operations should be on-going in order to identify possible operational potential as appropriate. This chapter does not cover cyber investigations; refer to reference (k) for details on cyber specific investigations. However, cyber forensics and applicable cyber investigative or operational activities should always be considered during national security investigations and early coordination with the Cyber Field Office is encouraged.

20-7. National Security Investigations

a. This chapter focuses on NSIs in which there is either:

(1) A specific and articulable reason to believe a "DoD-affiliated person" has committed, attempted to commit, or intends to engage in espionage, sabotage, illicit technology transfer, treason, sedition, assassination, or terrorism, or otherwise poses a threat to National Security, or

(2) A specific and articulable reason to believe a non "DoD-affiliated person" poses a foreign intelligence or terrorist threat to the DON or DoD components supported by NCIS including personnel, assets, and technologies, or

(3) A report or allegation which falls within the DON's Suspicious Activity (5Y) or Reportable Indicator (3Y) requirements but does not provide sufficient "reasonable belief" to predicate a full NSI. These investigations are considered "preliminary" and should be resolved within 120 days or changed to a different "full field" National Security case category.

b. National Security Case Categories. See Appendix B for associated violations and Appendix C for a crosswalk showing types of investigations.

(1) Technology Transfer (3T, formerly 5A) - Used for investigations involving the suspected unauthorized transfer of technology equipment, information, or material which can be used or adopted for use in the design, development, production, maintenance, or reconstruction of critical military systems by hostile or potentially hostile countries either directly or through third countries.

(2) Espionage (3C) - Used for investigations involving the suspected unlawful obtaining, delivering, transmitting, communicating, or receiving of information pertaining to the national

defense with the intent or reasonable belief the information may be used to injure the U.S. or benefit a foreign nation.

(3) Foreign Contact (3D) - Used for investigations regarding DON personnel who have self-reported contact (either in person, by telephone, by email, or by any other form of communication) with a suspected or known FIE.

(4) Leakage (3L, formerly 5E) - Used for investigations involving the deliberate unauthorized release of classified information into the public domain, such as through media disclosure which is not officially sanctioned or cleared. Reference (l) provides specific reporting requirements and as such these cases can only be opened with the approval of NCISHQ NSD.

(5) Sabotage (3F) - Used for investigations of any act of willful damage or destruction of any national defense or war material, premises, or utilities, with intent to injure, interfere with, or obstruct the national defense. Usually begins as a criminal case (6U) but changes to this case category when the intent is associated with a threat to the national defense. This case category is covered within reference (m).

(6) Insider Threat (3I) - Used to report on investigative information and/or activities that result from credible reports of willful compromise or willful unofficial disclosure to unauthorized persons of classified information, or multiple insider threat indicators including but not limited to confirmed unreported foreign travel and unreported FIE contacts, by individuals with placement and access to classified information, controlled technologies, or military facilities/programs.

(7) Reportable Indicator (3Y) - Used to report investigative activities based on information provided under the DoD/DON Personnel/Information Security program by reference (f) and provided in Appendix C, but which initially does not provide enough indicators for a 3I or sufficient reasonable belief to initiate a 3C or other NSI case category.

(8) Terrorism (5T) - Used for investigations of suspected domestic or international terrorism activities.

(9) Suspicious Incident (5Y) - Used to report investigative activities based on information provided under the DoD suspicious incident reporting requirements, reference (n), but which initially does not provide enough indicators or sufficient reasonable belief to initiate a 5T terrorism investigation.

20-8. Jurisdiction

a. The documents listed as references provide NCIS its jurisdictional boundaries for counterintelligence and terrorism investigations, as well as set forth the jurisdiction of the various CI components of the U.S. and requirements for coordination with the Federal Bureau of Investigations (FBI) inside the U.S. and with the Central Intelligence Agency (CIA) and other appropriate intelligence/CI components outside of the U.S. The crosswalk enclosure provided in

Annex C of reference (o), provides a detailed delineation of lead investigative responsibilities for domestic terrorism (DT), international terrorism (IT), and counterintelligence (CI) investigations.

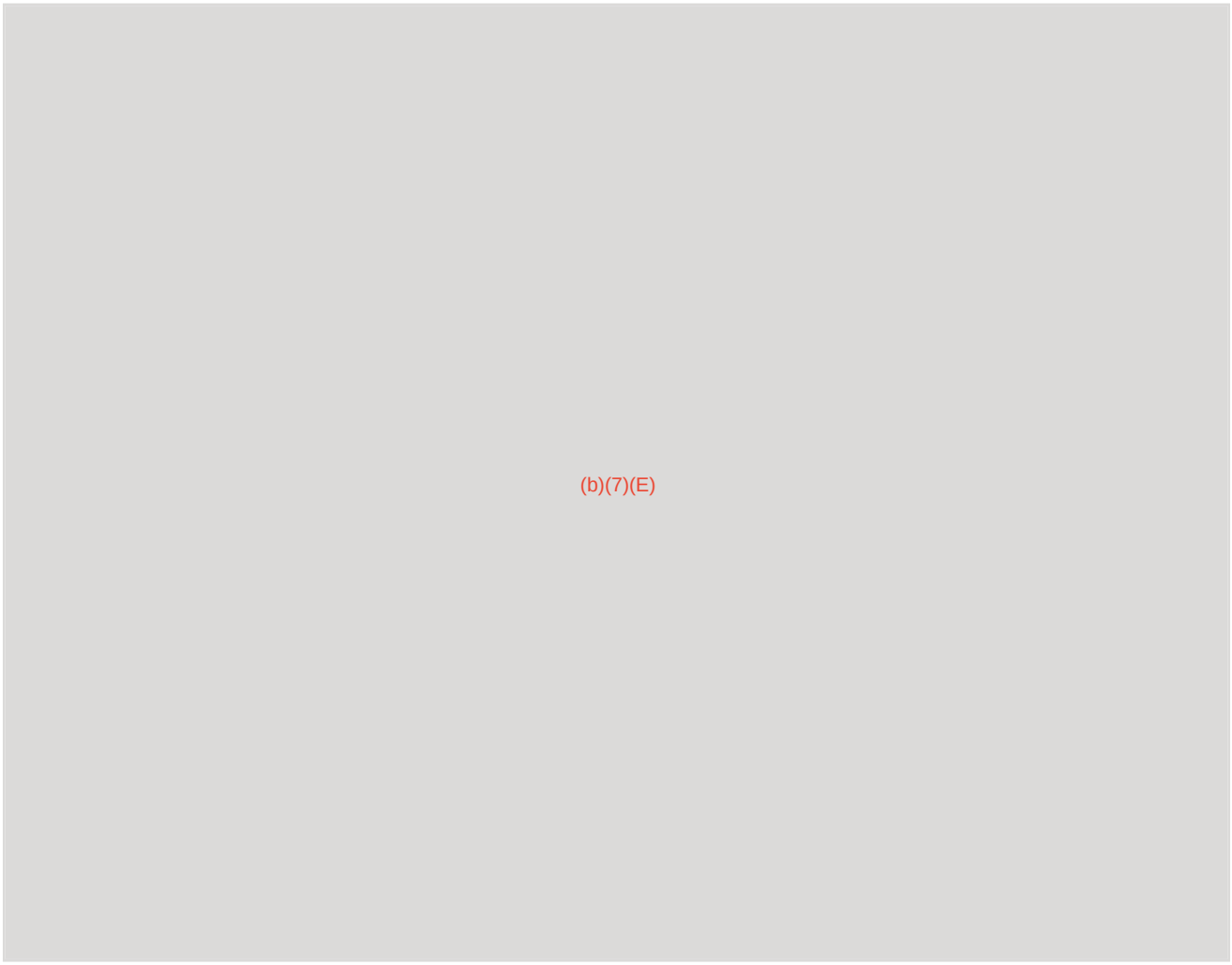
(1) NCIS has primary jurisdiction in CI (non-terrorism) investigative matters pertaining to active duty members of the Navy or the Marine Corps in and outside the U.S. When the investigation concerns retired military personnel, or active or inactive reservists, NCIS has primary jurisdiction only if the alleged violation occurred while the subject was on active duty. DoD and some command elements may conduct CI Inquiries per the requirements and restrictions outlined reference (p); however, NCIS is the only DON organization authorized to conduct CI Investigations and certain investigative techniques. In these situations, NCIS needs to ensure that there is early coordination between the Department of Justice (DOJ) and DON on the venue for possible future prosecution. Additionally, there are two exceptions to the active duty rule. The first is an investigation of alleged violations occurring while the DON member was assigned to a U.S. diplomatic mission abroad. The FBI has primary jurisdiction in the diplomatic mission areas under section 603 of the Intelligence Authorization Act of 1990. Those missions include embassies, consulates general, consulates, and consular agencies. The second is an investigation of violations of the Atomic Energy Act of 1946, regardless of the status or location of the subject.

(2) The FBI has primary jurisdiction on all terrorism related investigations inside the U.S. no matter the military status of the subject of the investigation. NCIS maintains primary jurisdiction over active duty Navy or Marine Corps members outside the U.S. The FBI has primary jurisdiction for all CI and terrorism investigations of foreign nationals within the U.S. and on all civilian personnel, including DON civilian and contract personnel. All FBI investigative activities must be conducted consistent with the Attorney General Guidelines for Foreign Intelligence Collection and Counterintelligence Investigations. Although not always the lead investigative agency and in accordance with reference (c), NCIS has the authority to vigorously investigate and collect information on any person, organization, group or situation involving suspected intelligence, terrorism or criminal activities when that person(s), organization or group is DON-affiliated and/or the situation to be investigated or collected upon is one in which, regardless of suspect status, a clear threat of victimization to the DON is present.

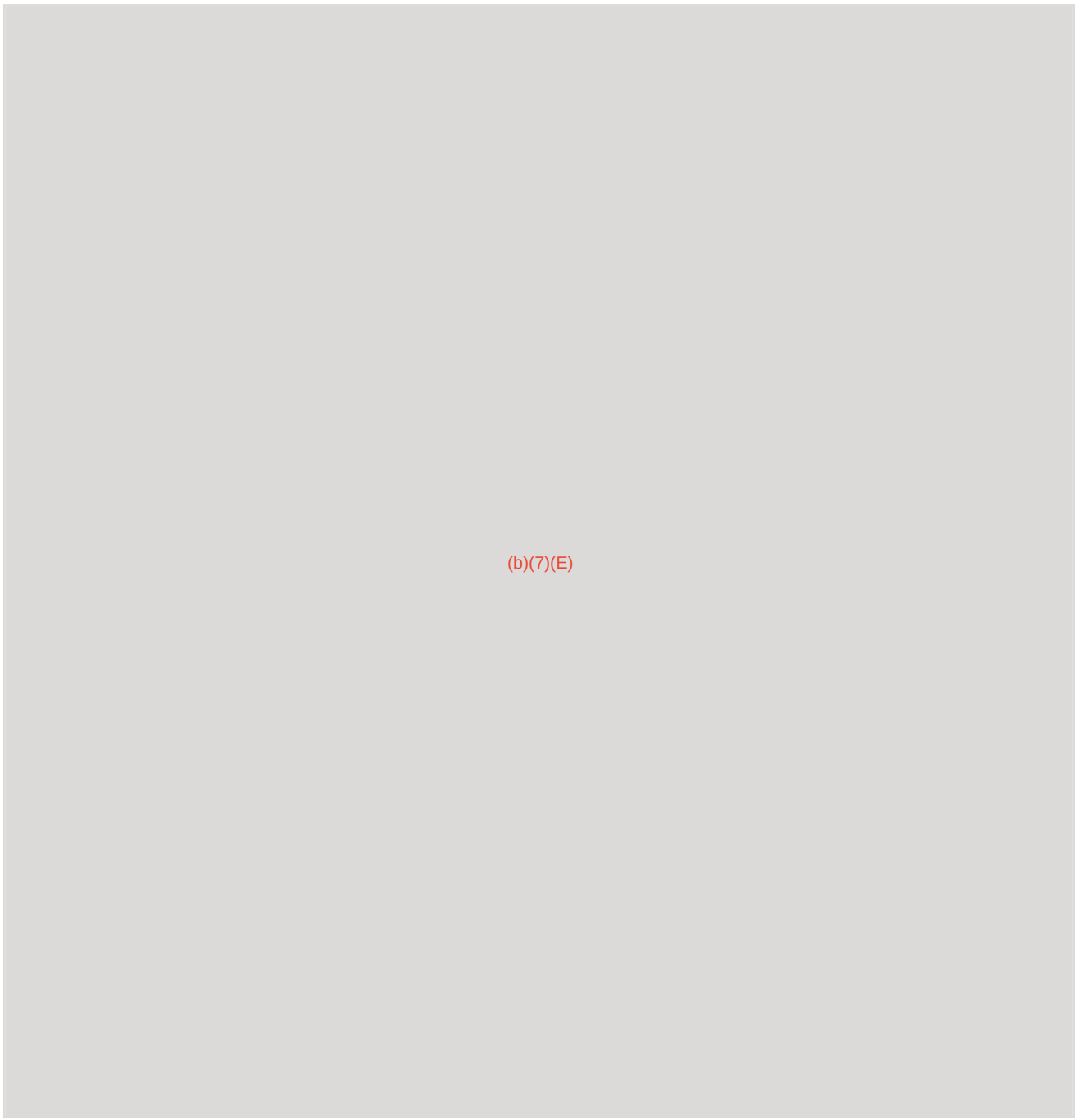
b. The FBI is the primary agency with which NCIS will coordinate espionage and terrorism investigations within the U.S. Determining which agency is the lead or supporting agency depends on the type of investigation, military or civilian status of the subject of the investigation, and the permanent location of the subject (foreign or domestic).

(1) NCIS special agents and supervisors should be familiar with the DoD/FBI MOU identified in reference (o) and all associated current annexes. These annexes outline requirements for information sharing and coordination associated with counterterrorism and counterintelligence activities. Although the annexes and references delineate investigative responsibilities among the various CI components, partnership and cooperation are the keys to successfully conducting these complex and vital investigations in an effort to bring about the desired results, whether prosecutorial, administrative, or resultant in spin-off operational activity.

(2) Field elements of the FBI and NCIS should maintain strong working relationships and meet frequently for the purpose of ensuring close cooperation in order to effectively carry out their CI authorities. Additionally, NSD and FBIHQ should also maintain productive relationships in order to ensure that the requirements for notification are made in a timely and accurate manner. Per the DoD/DOJ MOU, notification to the appropriate MDCO of an investigation involving DoD interest is required. Both NCISHQ and FBIHQ are required to notify the other via letterhead memorandum when an NSI indicates that classified information is being or may have been disclosed in an unauthorized manner to a foreign power or an agent of a foreign power. This notification is known as a "Section 811 notification," and is the responsibility of the NSD desk officer. Appendix E provides amplifying information. If the FBI waives jurisdiction, NCIS may take investigative actions necessary to corroborate or refute the allegations in an effort to protect the security of DON personnel, information, activities, materials, and installations. Since NCIS is exclusively assigned on behalf of the DON to maintain liaison on all terrorism, counterintelligence and security matters with Federal law enforcement, security and intelligence agencies, it is inferred the FBI will not unilaterally conduct an investigation involving a DON command or member without NCIS notification and participation.



Pages 558 through 560 redacted for the following reasons:
- -
(b)(7)(E)



20-12. Technology Transfer (Category 3T)

a. This case category is used for investigations involving the suspected unauthorized transfer of technology equipment, information, or material which can be used or adopted for use in the design, development, production, maintenance, or reconstruction of critical military systems by hostile or potentially hostile countries either directly or through third countries.

(1) Technology transfer can be defined as the unauthorized transfer of technology, equipment, or information which can be used or adapted for use in the design, development, production, maintenance, or reconstruction of critical military systems by hostile or potentially hostile countries, either directly or through third countries.

(2) One of the most advantageous "force multipliers" in any conflict is the utilization of superior military technology. Clearly, the optimal method for an adversary to gain technological parity or superiority with the U.S. is to acquire our technology. Obtaining our technology serves several purposes: first, the acquired technology can be directly utilized to develop weapons systems equal in capability; second, it can be enhanced to provide a superior technological edge; and third, it can be exploited to facilitate the development of countermeasures, thereby mitigating capabilities in a conflict.

(3) Illegal technology transfer investigations do not require the technology to be classified in nature; actually many successful prosecutions have focused on unclassified export controlled technologies that may be commercially available but are restricted from use by certain countries for military purposes. As such, an adversary is often able to obtain controlled military components via what initially appear to be "legitimate" purchases. The majority of U.S. commercial exports do not require a license. Authorization to export is determined by the transaction: what the item is; where it is going; who will receive it; and what it will be used for. There are restrictions on some commercial unclassified products being provided to certain restricted countries. Technology transfer may be accomplished through acquisition of open source material, fraudulent exportation, diversion of embargoed material into illegal trade channels, or traditional clandestine means. In addition, although the end user of the transferred technology may be a foreign entity, suspect persons or organizations are often U.S. persons and are afforded the appropriate protections under references (a) and (c).

(4) Early engagement with the NCISHQ Research, Development, and Acquisition (RDA) analysts is highly beneficial when conducting technology transfer investigations. Additionally, information collected should be reported via IIR, as long as it does not jeopardize ongoing investigative activity or prosecution. Once an investigation is closed and/or the prosecution completed, the case file should be reviewed for information that should be disseminated via IIRs in response to standing collection requirements.

(5) The best defensive vehicle to mitigate the transfer of U.S. technology is the provision of awareness briefings to make the threat known to those individuals involved in the research, development, testing, or production of information or equipment using critical emerging technologies. These briefings should detail the various collection methodologies outlined in this chapter, as well as provide insight into the specific technologies that are being targeted and identify the companies being used to facilitate foreign collection. Care should be taken to ensure that any information briefed does not compromise ongoing investigative or operational efforts. Reference (u) provided additional requirements associated with NCIS CI support to RDA.

b. Transfer of Munitions. Previous guidance for investigations covering illicit munitions transfer directed the initiation of a Category 3T investigation only if FIE involvement was indicated. However, since intelligence activity is often conducted clandestinely to insulate state

sponsorship of technology transfer, FIE involvement is not always apparent at the onset of an investigation. This chapter now directs that even if FIE involvement is not initially identified, investigations involving the illegal export of restricted commodities from the U.S. will be opened as a 3T with NSD oversight. The NCISHQ Criminal Investigations Directorate (Code 23) will oversee all investigations involving the illegal import of restricted items (to include munitions, narcotics, etc.) into the U.S. Moreover, investigations into the transfer of weapons, armaments, or other material support to a designated terrorist organization inside or outside the U.S. will be conducted under the 5T case category.

c. Transfer of Classified Technology. If the technology being transferred is classified and involves a subject in contact with a foreign intelligence entity, NSD may direct that the case category be changed to an espionage (3C) investigation and possibly transferred to OSP.

d. Investigative Coordination and Activities

(b)(7)(E)

(b)(7)(E)

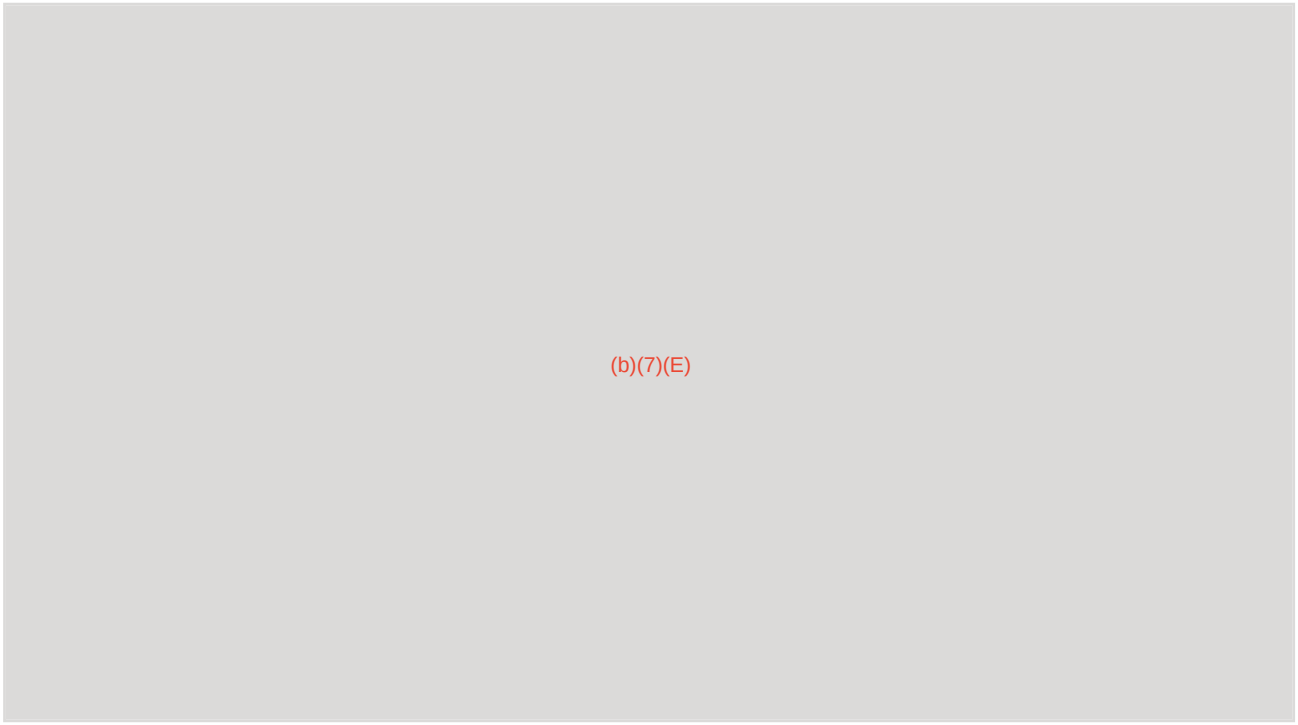
20-13. Espionage (Category 3C)

a. This case category is used for investigations involving the suspected unlawful obtaining, delivering, transmitting, communicating, or receiving of information pertaining to the national defense with the intent or reasonable belief the information may be used to injure the U.S. or benefit a foreign nation. The specific laws concerning this activity are set out in Title 18, U.S. Code, Sections 793-798, Title 50, U.S. Code, Sections 436 and 783, and Title 10, U.S. Code, Chapter 47 Uniform Code of Military Justice (UCMJ), Article 106A. The special agent's study of Federal statutes and Article 106A of the UCMJ will identify the elements, which must be proven for any successful espionage prosecution. Appendix P provides some key elements to include in a subject's statement in an espionage investigation. Additionally, because of the broad scope of the Espionage Act, many instances of compromise and unauthorized disclosure may simultaneously amount to other criminal violations.

(1) Even if the investigation does not identify a foreign connection, there are severe penalties prescribed for a willful communication of defense information to unauthorized recipients, the loss or unauthorized disclosure of defense information through gross negligence, or the failure to report a known loss of defense information. Generally, an espionage investigation will address the elements needed to prosecute these lesser charges, but the investigator must be aware of their importance and the evidence required for proving them in either Federal or military court.

(2) Additionally, it is essential that suspects be properly advised of their rights in accordance with Article 31(b), UCMJ, or the Fifth Amendment of U.S. Constitution, as appropriate. Guidance for a proper advisement of rights can be drawn from the applicable section of the Espionage Act. Appendix B provides additional information on violations associated with "The Unlawful Solicitation, Acquisition, Possession, Disclosure, and Communication of National Defense or Classified Information." Consultation with assisting government, military, and/or NSLU attorneys can assure these lesser charges are identified and the corroboration needed is completely understood.

b. Investigative Coordination and Activities



20-14. Foreign Contact (Category 3D)

a. This case category is used to document investigative activity associated with an individual who voluntarily self-reports a foreign contact (either in person, by telephone, by email, or by any other form of communication) with a suspected or known FIE. This case category should also be used in place of the previous 3G "Information Request" when the information requested is believed to be from a hostile intelligence agency and is targeting an individual who self-reports the contact. See 3Y or 5Y for documenting receipt of suspicious requests for information or base access that do not meet the criteria for a 3D. The DON Personnel Security Program Regulation, reference (i), which requires DON personnel to report such contacts to NCIS, specifically states: "All personnel who possess a security clearance are to report to their commanding officer, activity head, or designee, contacts with any individual, regardless of nationality, whether within or outside the scope of the individual's official activities in which illegal or unauthorized access is sought to classified or otherwise sensitive information. Personnel must report to command if they are concerned that they may be the target of exploitation. The commanding officer will review and evaluate the information and promptly report it to the local NCIS office." Additionally, reference (f) requires all DoD personnel to report the contacts, activities, indicators, and behaviors identified in section 5 of reference (f) as potential FIE threats against the DoD, its personnel, information, material, facilities, and activities, or against U.S. national security to their organization's CI element. When CI support is not available, DoD personnel shall report the threat without delay to their security officer, supervisor, or commander. The security officers, supervisors, and commanders shall forward reported information to the MDCO (NCIS for the DON) within 72 hours.

b. This case category is to be used for the instance of the individual voluntarily coming forward to report the suspicious contact; as a result, a warning does not apply and should not be

given to the individual. However, a comprehensive debrief must be conducted and the operational potential should never be overlooked during the course of the debrief. At a minimum, the debrief should include a defensive briefing, instructions to report any follow-up contact, and the operational potential should be fully considered. The contact may be as a result of legitimate travel, work, social, or family, but the investigation should be sensitive to the fact that DON personnel may be an unwitting party to a foreign intelligence activity. This case category can also be used as a follow-on to a 9F (Foreign Travel Brief/Debrief) when an individual has provided information in the debrief that indicates possible follow-on or continuous contact with a possible FIE. The investigation should be initiated with the foreign national as the subject (S/) of the investigation and the "victim" (V/) being identified as the self-reporting DON person. This will enable certain investigative activities to be levied on both the S/ and V/ in order to fully identify the nature of their relationship. In all instances, the investigation will at the very least determine the position the self-reporting individual holds, the level of his/her clearance and access, the exact nature, form and circumstances of the contact, and all available identifying information on the foreign national including (where applicable) complete physical description.

c. This case category should not be used for "unreported" or third party reported foreign contact reports. Additionally, this case category should not be used for individuals who admit to a previously unreported foreign contact only after being confronted by a failed or pending polygraph. In instances where the command or NCIS becomes aware of the contact through other than voluntary self-reporting, prudence dictates a more cautious approach because the failure to report the contact by those individuals who have a reporting requirement may constitute a punishable offense for violation of a general order or regulation. Reference (f) provides that persons subject to chapter 47 of title 10, U.S. Code, referred to as the Uniform Code of Military Justice (UCMJ), who violate specific provisions of this issuance may be subject to punitive action under Article 92, UCMJ; and that civilian employees under their respective jurisdictions who violate specific provisions of this issuance may be subject to appropriate disciplinary action under regulations governing civilian employees. As such, the motive for the contact and the reason for not disclosing becomes a paramount consideration and the initiation of a 3I is recommended. If there is any substantive indication that the motive is espionage or support to terrorism, consideration should be given to initiating a 3C Espionage or 5T Terrorism investigation (see paragraph 20-19).

20-15. Leakage (Category 3L)

a. This case category is used for investigations involving the deliberate unauthorized release of classified information into the public domain, such as through media disclosure which is not officially sanctioned or cleared. Utilized for incidents involving the appearance of classified information in the public media, leakage is a special type of "unauthorized disclosure" complicated by the widespread public compromise of the information concerned. Typically, such investigations result from the appearance of information considered classified in a newspaper, magazine, book or trade publication, online publications or in social media, or the verbal/visual disclosure of such data during a radio or television broadcast. An investigation is based upon the presumption that one or more individuals, in lawful, authorized possession of the

classified defense information, communicated or "leaked" such data to someone who, in turn, published or circulated the material in the public media. Leakage investigations may only be authorized by NSD and must meet the requirements set forth in reference (l) prior to initiation of an NCIS leakage investigation. Leakage investigations are different from "spillage" investigations. "Spillage" investigations are considered a cyber-related event and are covered under reference (k).

b. Leakage investigations by NCIS are normally initiated at the seat of government (SOG) level, not by NCIS field components at the request of a local command. This is due to particular SOG procedures pertaining to leakage matters (set forth below) that are designed, in part, to ascertain whether the information in question is actually classified or has been previously released for publication. Accordingly, in most leakage situations, it is preferable to complete the SOG procedures prior to initiating an investigation. Leakage investigations are frequently complex, involve highly sensitive information, and invoke public interest; liaison between the field and HQ is encouraged on all aspects of these investigations, including whether initiations should be in the field or at HQ. In the event a field or NSD component receives a leakage complaint but determines that additional command action is required according to reference (l), the component shall expeditiously report the matter by ROI (INFO). NCISHQ will then coordinate with the Deputy Undersecretary of the Navy's office concerning the SOG procedures.

20-16. Sabotage (3F). This case category is used for investigations of any act of willful damage or destruction of any national defense or war material, premises, or utilities, with intent to injure, interfere with, or obstruct the national defense. These cases usually begin as a criminal case (6U) but change to this case category when the intent is associated to a threat to the national defense. This case category is covered under reference (m).

20-17. Insider Threat (3I)

a. This case category is used to report investigative information and/or activities that result from credible reports of willful compromise, willful unofficial disclosure to unauthorized persons of classified information, or multiple insider threat indicators including but not limited to confirmed unreported foreign travel and unreported suspected FIE contacts, by individuals with placement and access to classified information, controlled technologies, or military facilities/programs. This case category can also be used for initial CI investigations into individuals with a Top Secret clearance and/or access to sensitive programs that commit suicide, go missing, or desert to a foreign country. The initial information may not always provide sufficient "reasonable belief" to predicate an espionage investigation; however, this case category can be used to "seek to resolve an allegation or information indicating a potential threat to national security," but which does not initially predicate an espionage investigation. ROI (INFO) reporting will be used by NSD Investigations or NSD Analytical Division to document insider threat assessments and subsequent recommended actions to the field elements or declinations to a referring agency.

b. Unauthorized Disclosure/Willful Compromise (Formerly 5D)

(1) As provided in the espionage section of this chapter, there are significant Federal and UCMJ penalties associated with the willful, unofficial disclosure of classified information to unauthorized persons. Such conduct is a violation of security regulations, and may amount to an offense punishable under Title 18, U.S. Code 793. The statute provides severe criminal penalty for persons either in lawful or unauthorized possession of defense information who willfully communicate, deliver, or transmit such data to any person not entitled to receive it. Examples of unauthorized disclosure include: verbal relaying of classified information to an unauthorized recipient; showing a classified document to an unauthorized person, or the inclusion of classified data in a personal letter or email to a friend or relative. These investigations should reflect, as far as possible, the precise (verbatim if possible) information that is suspected of being wrongfully disclosed.

(2) It is mandatory that NSD be promptly notified in all matters pertaining to possible unauthorized disclosure/compromise of sensitive compartmented information (SCI), special access program (SAP) information, and/or information regarding intelligence sources and methods. Additionally, NSD should be immediately notified if the unauthorized disclosure is to a representative of a foreign government or a known or suspected FIE officer or agent. Such investigations should be initiated as a 3C.

c. Unreported Foreign Contact and Unreported Foreign Travel

(1) For those individuals required to report, unreported foreign contacts especially when associated with unreported foreign travel are of significant concern and should be thoroughly investigated in an effort to identify any FIE involvement or national security threat. This case category should be used for initial "unreported" or third party reported suspicious foreign contact/travel reports including investigations involving individuals who admit to a previously unreported foreign contact only after being confronted by a failed or pending polygraph. In instances where the command or NCIS becomes aware of the contact through other than voluntary self-reporting, prudence dictates a more cautious approach because the failure to report the contact by those individuals who have a reporting requirement may constitute a violation of a general order or regulation, that is punishable under Article 92 of the UCMJ for Navy/Marine Corps personnel. Additionally, the DON Personnel Security Program Regulation similarly binds Navy civilian personnel, and, although their failure to report such contact cannot be prosecuted in a court of law, the failure to report can result in administrative/disciplinary action. As such, the motive for the contact and the reason for not disclosing the contact and travel becomes a paramount consideration and the initiation of a 3I is recommended. If there is any substantive indication that the foreign contact is a suspected or known FIE, consideration should be given to initiating a 3C Espionage investigation.

(2) Experience has shown that oftentimes the contact that has not been reported is still legitimate but cannot be so assumed at the outset. Additionally, it is important to determine the reporting requirements of the individual since those requirements may differ based on clearance level, command, and military status. One investigative protocol used successfully and that should be utilized whenever feasible, is to insure the individual attends a scheduled command CI awareness briefing in order to preclude a subsequent claim that he/she was unaware of the

requirement to report contact. This protocol has resulted in a subject coming forward after the awareness brief to report some form of non-hostile contact. If the awareness brief does not resolve the issue, consideration is given to the careful recruitment of sources that have existing contact with the individual. A supervisor, roommate, or co-worker might be co-opted to accept specific tasking to help resolve the individual's motive. Depending upon the circumstances, pretext interviews of associates have sometimes been effective in resolving the individual's motive.

(3) As a final step, the DON military suspect should be afforded an Article 31(b) warning; suspected of failure to report, as required by the Naval Personnel Security Program Regulation, a suspicious contact or a contact with a hostile country representative. He or she should be thoroughly debriefed without disclosing any sensitive sources or methods. Polygraph examination should always be considered. In those infrequent instances involving DON civilian personnel, failure to report a contact is not a violation of any U.S. Statute and absent a custodial interrogation, there is no requirement to provide a Miranda warning. Should a polygraph examination of the DON civilian become necessary, Miranda warnings will be required in compliance with DOD/NCIS policy. NCISHQ will authorize polygraph in these instances upon completion and reporting of in-depth interview vice interrogation of the suspect. In order to comply with DOD policy, the suspect must be afforded a Miranda warning at the time of and incidental to the polygraph examination.

d. Desertion/Missing Persons Considerations

(1) There are other situations warranting investigation under the 3C or 3I case category given possible espionage indicators. They include, but are not limited to, DON personnel with a Secret or above clearance expressing the intention or circumstances indicating defecting to a foreign country or DON personnel with highly sensitive access in the intelligence or communications specialties being absent or missing without explanation and the circumstances of their absence. 3I investigations involving a missing person should be worked in coordination with NCISHQ Code 23 and using Category 7M protocols as provided in reference (w). Reference (f) requires that commands notify NCIS concerning actual or attempted cases of defection. Upon receipt of information concerning suspected defection by DON personnel, the NCIS component shall open a 3I investigation in order to determine if a defector situation does exist.

(2) Defector investigations should include the following:

(a) Determine the subject's clearance status and actual access,

(b) Determine if any classified material is missing,

(c) Encourage the command to issue a DD Form 553, “Deserter/Absentee Wanted by the Armed Forces,” in a case of Navy or Marine Corps personnel for immediate apprehension and enter the subject as a deserter in National Crime Information Center (NCIC),

(d) Initiate appropriate border alerts if feasible,

(e) Interview co-workers, friends and acquaintances to determine the reason for the defection/unexplained absence,

(f) Determine any action taken to effect the defection such as destruction of uniforms and ID cards, use of fictitious names and identification papers, and

(g) Determine any known connections with foreign persons or organizations.

(h) Request National Security Letters be issued to financial institutions to determine current location or future travel plans, among other information.

(3) If the subject is apprehended, cancel the NCIC entry and any initiated border alerts and interrogate the subject. The Article 31(b) warning should cite the offense of desertion (not defection), a violation of Article 85, UCMJ. The warning should also address any other violations developed during the course of the investigation. The NCIS agent should attempt to obtain a sworn statement, documenting the reasons for the desertion (attempted defection) and identifying any other persons who encouraged the subject's actions. If the investigation involves a civilian employee, Miranda warnings need only be provided if the individual is in custody or otherwise subject to a custodial interrogation. When an investigation establishes a reasonable belief that an individual, whether civilian or military, has provided or is providing classified information to a foreign power or agent thereof without authorization, notification must be provided to FBIHQ in accordance with 50 U.S.C. Section 402a. Such notification is provided by NCISHQ.

20-18. Reportable Indicator (3Y) **.** This case category is used to report investigative activities based on information reported under the DON Personnel/Information Security Program or by reference (f) and provided in Appendix C, but which initially does not provide enough indicators for a 3I including a willful act by a person with placement and access to classified information, or sufficient reasonable belief to initiate a 3C or other NSI case category. Like the 3I, this case category can be used to resolve an allegation or information indicating a potential threat to national security, but which does not meet the reasonable belief standard. However, these investigations should be either resolved within 120 days or changed to one of the above NSI case categories. If gross negligence or intent to compromise classified information is identified, the investigation should be worked as a 3I or 3C since Title 18, U.S. Code 793 provides penalties for persons entrusted with the possession or control of defense information and who permit it to be lost, stolen, abstracted, or destroyed through gross negligence or fail to make a prompt report of such known loss. All 3Y investigations shall have senior management concurrence before closure.

a. Suspicious Information Request (formerly 3G). The 3Y should be used in place of the previous 3G “Information Request” when the information requested is suspicious but does not provide enough information to support a 3I, 3C, or 3D.

b. Mishandling Violations/Loss Of Classified (formerly 5F/5B)

(1) The 3Y should be used in place of the previous 5F "Compromise" as it covers "access to classified material by unauthorized person(s) as a result of mishandling of classified material." Such investigations include the following complaints: damage/loss in transit, inadequate protection, classified material found adrift, and unauthorized or incomplete destruction.

(2) The 3Y should be used in place of the previous 5B "Loss of Classified Matter" when documenting investigative activities associated with classified material that is out of the control of its custodian and cannot be located when sought (mysterious disappearance/misplacement).

(3) Loss of classified due to a break-in should also be investigated under a 3Y, unless there is information that the break-in is associated to an individual with placement and access or is associated with an FIE. Investigations associated with a break-in should be coordinated with Code 23.

c. Analytical Assessment. Under this case category, an ROI (INFO) can also be used to document insider threat referrals which result in an NCIS analytical insider threat assessment but do not meet the threshold for a CI investigation.

20-19. Joint Terrorism Task Force And Terrorism (5T)

a. As provided previously in section 20-8, and detailed in reference (o), the FBI has primary jurisdiction within the U.S. on all terrorism investigations. In the wake of September 11, 2001, the Joint Terrorism Task Force (JTTF) became the primary operational and investigative arm of the U.S. Government in counterterrorism matters. References (x) and (y) designated the FBI as the lead U.S. agency in preventing and investigating acts of terrorism, as well as coordinating the efforts of all law enforcement agencies. These directives and the JTTF program ensure a vigorous response to prevent, disrupt, and mitigate all terrorist threats or attacks within the U.S. or against U.S. citizens overseas. In July 2002, the FBI Director established the National Joint Terrorism Task Force (NJTTF) to address the complex information sharing, coordination and logistical issues with operating multi–agency task forces. The mission of the NJTTF is to enhance communication, coordination and cooperation between Federal, State, and local government agencies representing the intelligence, law enforcement, defense, diplomatic, public safety and homeland security communities by providing a "point of fusion" for the effective sharing of terrorism intelligence and by managing the JTTF program nationwide through direct administrative, training, and policy oversight. The NJTTF consists of more than forty government agencies and is co-located within the National Counterterrorism Center (NCTC). The NCIS has special agents and analysts assigned as Task Force Officers (TFO) to FBI field office JTTFs and the NJTTF to ensure the timely sharing of all threat, indications and warnings (I&W), and investigative information pertaining to the DON. The TFOs are administratively controlled by their local NCIS field office, but operationally controlled by the FBI JTTF SSA. NCIS representatives assigned to the NJTTF work for NSD and ensure NCIS senior management and the MTAC are advised of imminent threats or emerging terrorism information pertaining to the DON.

b. TFO Roles and Responsibilities

(1) Reference (z) provides details as to the roles and responsibilities of a TFO and outlines the agreements made between NCIS and the FBI in regards to assigning a TFO including the chain of command, length of assignment, TFO level of expertise, release of information, and material support. NCIS TFOs receive logistical support from both the FBI/JTTF and their local field office. The JTTFs provide TFOs with their required standard office supplies and space including an FBI cell phone, computer, and locally held investigative equipment. NCIS will still provide the TFO with all required NCIS space and IT support needed to meet NCIS administrative requirements including, but not limited to, online training, communications, SLDCADA, etc. NSD will also provide some personal protection and investigative equipment as required. The NCIS field office will provide the NCIS TFO with a U.S. Government vehicle; and its use, including domicile-to-duty (DTD) approval, will be consistent with the needs of the FBI JTTF (the FBI cannot provide vehicles to other Federal LEAs). NSD will identify and facilitate any required NCIS sponsored training, as well as outside relevant training consistent with NCIS Code 10 protocols and budgetary concerns.

(2) As provided in reference (z), for day-to-day operational matters, individuals assigned to a JTTF will be under the supervision of their respective JTTF supervisor, normally an FBI SSA. However, all NCIS personnel assigned to a JTTF are obligated to keep NCIS field office senior leadership and NSD apprised of all DON nexus operational and investigative activities. Additionally, reference (o) provides requirements for information sharing and coordination by the FBI as it relates to DON related investigations. Notifying a TFO of a DoD nexus investigation does not constitute notification to the affected Service, nor does it constitute a joint investigation.

c. Terrorism (5T)

(1) This case category is used to investigate suspected domestic or international terrorism activities. A terrorism investigation is defined in reference (o) as "Investigative activities undertaken to determine whether particular persons are acting for or on behalf of, or if an event is related to, an organization, group, or person engaged in domestic or international terrorism, and to determine actions required to neutralize such acts."

(a) Domestic Terrorism (DT): "Activities that occur primarily within the territorial jurisdiction of the U.S. that involve violent acts or acts dangerous to human life that are in violation of the Federal or State criminal laws, and that appear to be intended to intimidate or coerce a civilian population in the U.S., influence the policy of a government in the U.S. by intimidation or coercion, or affect the conduct of a government in the U.S. by mass destruction, assassination, or kidnapping." Consultation with NSD and NSLU, or both, should be conducted prior to initiating a 5T associated with "domestic terrorism." These investigations are normally conducted jointly with the local FBI JTTF DT Unit and are expected to meet the above definition; otherwise the field office should consider a 5Y or initiation of the investigation utilizing a general crimes case category.

(b) International Terrorism (IT): "Activities that involved violent acts or acts dangerous to human life that are a violation of the criminal laws of the U.S. or of any State, or that would be a criminal violation if committed within the jurisdiction of the U.S. or of any State, and appear to be intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, or affect the conduct of a government by mass destruction, assassination, or kidnapping. These activities can occur outside or inside the U.S., or transcend national boundaries in terms of the means by which these activities are accomplished, persons they appear to be intended to coerce or intimidate, or locale in which their perpetrators operate or seek asylum."

d. Reporting Requirements

(1) Field office management teams are reminded that an investigation with a clear DON nexus (active duty member, DON employee or contractor, DON dependent) requires initiation of a Case Category 5Y (Suspicious Incident) and/or Case Category 5T investigation, as appropriate. Coordination with NSD should be conducted prior to initiating a 5T associated with domestic terrorism. If a Case Category 5T is initiated on a joint FBI/NCIS investigation, the field office should make every effort to assign a field office agent to work as the co-case agent with the TFO or FBI JTTF case agent. The NCIS investigation must adhere to NCIS reporting requirements; however, duplicative NCIS and FBI reporting is not desired. As a result, if the predominance of the investigation is being conducted by the JTTF members (including the NCIS TFO), then the ROI (INTERIM) can be used to:

(a) Indicate that an investigative action occurred by members of the JTTF and results of those actions are maintained in the FBI case file.

(b) Report on investigative actions (IAs) conducted by NCIS field office personnel (not the TFO) in support of the investigation.

(c) Send ACTIONS to other NCIS entities. If the local FBI office prohibits the opening of an NCIS investigative report, the field office management is encouraged to engage the local FBI management and NSD Investigations (22B) on the matter.

(2) A JTTF umbrella operation (XXJT) will be opened for each JTTF with NCIS personnel assigned. Appendix Q provides examples of the required reports associated with an XXJT. The purpose of the XXJT umbrella operation is to serve as a reporting vehicle to capture metrics and general NCIS activity relating to JTTF support that are not captured under a separate NCIS investigative case category. Using the umbrella operation, the NCIS TFO will provide a general identification and highlights of the investigations that they are supporting, the DoD nexus if available, and their activities conducted during that reporting period (i.e. surveillance conducted of subject). IIRs, NCIS case categories, and Guardian reports that resulted from the TFO's activities should be referenced in the XXJT. An XXJT ROI (INTERIM) will be submitted every 30 days and the operation summary at the end of the XXJT report must be completed with current month and fiscal year totals. The XXJT ROI (INTERIM) will be submitted to NCISHQ

in the format shown in Appendix Q. This report will provide field office and headquarters elements insight into the NCIS TFO's daily activities. However, the XXJT should not be used to provide a detailed report of the results of specific investigative or operational activity. TFO activities in support of a DON nexus investigation should result in the opening by the field office of a 5Y or 5T investigation.

(3) The requirements for Force Protection operations (XXFP) and other force protection related non-investigative activities are covered under reference (aa).

20-20. Suspicious Incident Reporting (eGuardian/5Y)

(b)(7)(E)

Pages 575 through 637 redacted for the following reasons:
- -
(b)(7)(E)

NCIS-3, CHAPTER 22
CI FUNCTIONAL SERVICES
EFFECTIVE DATE: MAY 2015

TABLE OF CONTENTS **PAGE**

22-1. Purpose. Per reference (a), NCIS is the Department of Navy Executive Agent for counterintelligence (CI). This chapter provides guidance on the conduct of counterintelligence functional services, including reporting, oversight, and management requirements. It establishes NCIS policy regarding responsibilities, requirements, and standards for prevention and detection efforts, including lead generation, that are conducted in support of other CI functions. References are provided in Appendix A. Appendix B contains a list of abbreviations and acronyms used throughout this chapter.

22-2. Policy. NCIS will conduct CI functional services according to the guidance in this chapter, and other chapters when appropriate, and in accordance with reference (a).

22-3. Cancellation. NCIS-3 Chapter 22, dated December 2006.

22-4. Chapter Sponsor. NCIS National Security Directorate (NSD), Code 22.

22-5. General Information

a. In accordance with references (b) and (c), CI functional services encompass CI activities that support other intelligence or Department of Defense (DoD) operations by providing specialized CI services, such as technical surveillance countermeasures and support to critical technology protection, to identify and counter the intelligence capabilities and activities of terrorists, foreign powers, and other entities directed against U.S. national security. Reference (d) further defines CI functional services as CI activities that are not unique to the other CI functions, that support other CI functions and missions, and that include specialized services that are not inherently CI but support the CI missions and functions.

b. CI must first detect hidden foreign activities and work to develop a full picture of circumstances and events to be successful. The picture provides a platform for informed decision making, such as disruption, neutralization, or exploitation through investigative or operational activity. At its core, CI functional services is *a lead generation program* for other CI functions driven and informed by CI analysis. For example, awareness briefings are conducted to detect potential espionage or foreign intelligence entity (FIE) involvement, and debriefs are conducted to reveal operational potential and answer collection requirements.

c. One of the primary objectives of CI functional services is to establish the reasonable belief that a person is engaged in, or about to engage in, intelligence activities on behalf of a foreign power or international terrorist activities, or persons in contact with such persons for the purpose of identifying them and assessing their relationship. Establishing reasonable belief provides the basis for conducting a CI investigation.

d. CI in cyberspace. CI activities in cyberspace are fundamentally no different other investigations. The primary difference is through technical exfiltration of information the countering of which is covered in information assurance training and by technical security measures. It is important to remember that CI activities conducted by a foreign entity against a DoD person in the cyber realm should be handled the same as in the real world. For example, if a DoD employee or cleared contractor were to go to an academic conference in a country considered a CI threat, that person would get a defensive brief regarding the threat in that country. The same approach should be taken if the individual is attending a virtual conference on line. Threats among the participants should be identified and the appropriate defensive briefing should be given. The key is to heighten awareness. When traveling to a foreign country, awareness should naturally be heightened, however, when engaging in communication on line in your place of work it is easy to be lulled into a false sense of security. This adversary trying to lull you modus operandi sense of security is what needs to be countered.

e. The three general categories of basic CI functional services are espionage detection, support to military operations, and specialized services. This guidance focuses primarily on NCIS CI functional services support to local Security Inquiries (1L) and Special Inquiries (1X), found in Appendix C; Defensive Briefings (9F), found in Appendix D; Foreign Escort Briefings (9V), found in Appendix E; and CI and Insider Threat Awareness and Reporting Briefings (9Z), found in Appendix F.

f. A debriefing questionnaire for hosts and escorts of foreign visitors is provided in Appendix G.

g. A sample 9V ROI (OPEN) is provided in Appendix H.

h. The list of reportable contacts, activities, indicators, and behaviors is provided in Appendix I.

APPENDIX A
REFERENCES

(a) SECNAV Instruction 5430.107, Mission and Functions of the Naval Criminal Investigative Service, December 28, 2005

(b) DoD Instruction 5240.16, Counterintelligence Functional Services (CIFS), August 27, 2012, incorporating Change 1, effective October 15, 2013

(c) DoD Directive O-5240.02, Counterintelligence, December 20, 2007, March 17, 2015 (DoD PKI certificate required)

(d) DoD CI Functional Services Integrated Working Group Handbook, August 28, 2009

(e) DoD Manual 1348.33-V3, Manual of Military Decorations and Awards: DoD-Wide Performance and Valor Awards; Foreign Awards; Military Awards to Foreign Personnel and U.S. Public Health Service Officers; and Miscellaneous Information, November 23, 2010, incorporating Change 2, March 13, 2015

(f) Intelligence Community Directive 704, Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information, October 1, 2008

(g) Intelligence Community Policy Guidance (ICPG) 704.2, Personal Security Adjudicative Guidelines for Determining Eligibility for Access to Sensitivity Compartmented Information and other Controlled Access Program Information, October 2, 2008

(h) Director of Naval Intelligence ltr of 30 Apr 2009, Intelligence Community Directive (ICD) 704, Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information

(i) NCIS-1, Chapter 21, Personal Privacy and Rights of Individuals (Privacy Act), May 2008

(j) SECNAV Manual 5510.30, DON Personnel Security Program, June 2006

(k) DoD Instruction 2000.12, DoD Antiterrorism (AT) Program, March 1, 2012, incorporating Change September 9, 2013

(l) SECNAV Instruction 3850.2C, Department of the Navy Counterintelligence, July 20, 2005

(m) DoD Directive 5240.06, Counterintelligence Awareness and Reporting (CIAR), May 17, 2011, incorporating Change 1, May 30, 2013

(n) SECNAV Instruction 5510.37, Department of the Navy Insider Threat Program, August 8, 2013

APPENDIX B
ACRONYMS AND ABBREVIATIONS

CI	counterintelligence
CLEOC	Consolidated Law Enforcement Operations Center
CMS	Case Management System
CSR	Central Source Registry
DCII	Defense Central Index of Investigations
D-DEx	Law Enforcement Defense Data Exchange
DoDCAF	Department of Defense Consolidated Adjudication Facility
FIE	foreign intelligence entity
FN	foreign national
FV	foreign visitor
IA	Investigative Action
ICD	Intelligence Community Directive
ICPG	Intelligence Community Policy Guidance
IIR	intelligence information report
JPAS	Joint Personnel Adjudication System
K-Net	Knowledge Network
M3	U.S. Army Multimedia Message Manager
NCIC	National Crime Information Center
NLETS	National Law Enforcement Telecommunication System
OPM	Office of Personnel Management
OSS	Office of Strategic Support
PUR/E	employment and/or licensing check
SCI	Sensitive Compartmented Information
SOG	Seat of Government
SSO	Special Security Officer
TA	Threat Assessment
TAC	Tripwire Analytic Capability
TSCM	technical surveillance countermeasures
TWMS	Total Workforce Management System
USG	U.S. Government

Pages 642 through 666 redacted for the following reasons:
- -
(b)(7)(E)

CHAPTER 24
TITLE: FRAUD INVESTIGATIONS
POC: CODE 23A
DATE: SEP 07

24-1. INTRODUCTION.

24-1.1. This chapter provides general information important to the agent in conducting fraud investigations (Category 4). A detailed examination of fraud investigations is presented in NCIS-6, Manual for Fraud Investigations.

24-1.2. Fraud investigations are inherently complex and time-consuming. They require careful and detailed review of voluminous files and documents. The investigating agent must explore all relevant issues, be very thorough in his or her interviews/interrogations, and must maintain a firm grasp of all pertinent issues. Matters of investigative significance are often buried within a myriad of extraneous material. It is a great assistance to the investigation and disposition of fraud matters, as well as a sign of professionalism, to recognize and clearly report the relevant information while excluding unnecessary material. In other words, it is imperative that the investigation be "scoped" or

its parameters defined so that the investigation of specific, citable criminal statutes can be undertaken from the onset of the investigation.

24-1.3. When investigating fraud, the special agent will encounter complicated problems of law and administration, and will be confronted with technical problems that require recruitment and utilization of special training and skills. Coordination with a number of agencies and activities for technical assistance may be necessary.

24-2. DEFINITION AND ELEMENTS OF FRAUD.

24-2.1. Fraud Against the Government. Willful misrepresentations or concealment in order to obtain something of value from the government or to induce the government to part with something of value or to surrender a legal right.

24-2.2. Fraud is both a civil and criminal offense. Criminal fraud offenses are found under several sections in Title 18, United States Code (USC) and under various Articles of the Uniform Code of Military Justice (UCMJ), 10 USC 801, et seq. The victim of fraud, whether it is the government, a person, or a business, may pursue various administrative or civil remedies in place of, or in addition to, the criminal remedies. Sources of administrative government remedies include:

a. 5 USC 5512 (Withholding pay; individuals in arrears); and

b. DOD Instruction 7000.14-R, The Department of Defense (DOD) Financial Management Regulations.

24-2.3. Fraud against the government generally requires the following elements of proof:

a. A false representation, actual or implied; or the concealment of a matter of fact material to the transaction;

b. Knowledge of the falsity by the perpetrator.

Reliance and damages. The false information provided must be material to the contract in that more accurate or truthful information would have an impact on the acceptance of the contract. There must also be some form of damage to the party receiving the goods whether it be monetary, a reduced utility of the product received (product substitution is an example of this), or undue influence in accepting a bid that would not otherwise have been accepted (bribery, conflict of interest, kickbacks are examples of this). It should be noted reliance and damages, need not necessarily be proved when the government is the victim. They are, however, important in determining the amount of civil damages the government may later collect, and should not be ignored.

24-3. CATEGORY 4 INVESTIGATIONS. Investigations involving fraud are conducted under Category 4. Subcategories are as follow:

4A - Antitrust. Used for investigations of illegal anti-competitive activities involving any agreements or arrangements among competitors to limit competition.

4B - Credit Card Fraud. Used for investigations where there is a personal loss resulting from the illegal and unauthorized use of any credit cards, to include forgery involving credit cards, and other "access devices" defined in 18 USC 1029. This subcategory does not pertain to loss associated with government credit cards.

4C - Conflict of Interest/Standards of Conduct. Used for investigations pertaining to engaging in any private business or professional activity which would place DOD personnel in a position where there is a conflict between their private interests and the public interest of the United States. Gambling aboard government property or while on government duty is included in this subcategory.

4D - Defective Pricing. Used in investigations pertaining to a contractor's overpricing negotiated government contracts by quoting performance costs higher than those of actual expenditures or failure to provide all pertinent information regarding the true cost of the contract.

4E - Pay and Allowance. Used for investigations pertaining to false statements or other irregularities involving pay and allowance claims, reimbursement vouchers and improper disbursement of government funds. This subcategory will be used when investigating allegations involving unauthorized use of military benefits, to include: active, retired, reserve, and dependent AFID card abuse and medical benefits except those involving TRICARE.

4F - Personnel Actions. Used for investigations pertaining to fraudulent enlistments, appointments, examinations, advancements, discharges, separations, and falsification of personnel records or other personnel actions.

4G - General Procurement. Used for investigations pertaining to criminal or civil irregularities in connection with the procurement, administration, or disposition of U. S. Government property or services that are not otherwise specifically defined as a separate case subcategory.

4H - Bribery. Used for investigations pertaining to the offer and acceptance of bribes. A bribe is anything of value given, offered, or promised for the purpose of influencing official action.

4I - Dependency Assistance. Used for investigations pertaining to the service member's entitlement to dependency allowance for family members.

4J - Forgery (Personal). Used for investigations involving the forgery of checks uttered to persons and commercial institutions and the forgery of other documents where the government is not the victim.

4K - Forgery (Government). Used for investigations involving the forgery of checks, letters, orders for delivery of money or goods, receipts, military orders, identification cards, and property records when the U. S. Government is victimized. Also included are alterations of official documents, including personnel performance reports, certificates of training course completion, or test score results when reported officially.

4L - Subcontractor Kickbacks. Used for investigations pertaining to a subcontractor making any

payments, fees, commissions, credits, gifts, gratuities, or compensations of any kind to prime or to higher tier contractors or to any officer, partner, employee, or agent of higher tier subcontractors, or prime contractors.

4M - Cost Mischarging. Used in investigations when a contractor charges or attempts to charge the government for costs which are not allowable, not reasonable, or which cannot be either directly or indirectly allocated to the contract.

4N – Environmental Crimes. Used for investigations of any criminal violation of a federal, state, local, or foreign government statute designed to protect the environment.

4P - Product Substitution. Used in investigations when a contractor delivers, or attempts to deliver, to the government goods or services, which do not conform to contract requirements, without informing the government of the deficiency.

4S - Fraud Investigative Survey. This subcategory is used for an in-depth probe of a specific operation, activity, or program to determine if the systems being utilized are susceptible to criminal exploitation and if exploitation is present. The survey is not designed to take the place of investigations into known or suspected irregularities. NCISHQ approval is required before a survey may be initiated.

4T - Unauthorized Services (Government). This subcategory is used for fraudulently obtained services, i.e., minor automobile repairs and unauthorized gasoline purchases using a standard Form-44, where the government is the victim. The unauthorized or illegal use of all U. S. Government credit cards will be investigated under this category.

4U - TRICARE Claims Violations. Used for investigations pertaining to the falsification of documentation or unauthorized use of TRICARE.

4W - Workers Compensation (FECA). Used for investigations pertaining to false statements and claims made in order to obtain federal employee's compensation. This program is administered by the Department of Labor, Office of Workers Compensation Program (OWCP).

4X - Special Inquiry. Used for investigations having unique interests, requiring application of special investigative techniques or handling, occurring infrequently, or for other reasons not specifically covered by any other fraud subcategory. . This category will be utilized to investigate the theft of DOD identity cards that contain personal data. The theft of blank DOD identify cards will be investigated under the Category 6X. The initiation of an investigation regarding theft of ID cards will be left to the discretion of the Special Agent-in-Charge (SAC) when a "minimal" number of cards are involved.

4Y - Integrated Support Special Operation. Used to document the activities of Economic Crimes Integrated agents assigned to DON buying commands.

24-4. NCIS JURISDICTION.

24-4.1. In general, three factors govern jurisdiction: the laws and regulations that apply, the status of the suspect, and the geographical location of the offense.

24-4.2. There are three sources of laws and regulations that may apply to persons subject to military law and others who commit frauds against the United States. These are:

a. The Uniform Code of Military Justice (UCMJ) contains several articles that can be utilized during fraud investigations. The primary articles are Article 92 (failure to obey order or regulation), Article 132 (Frauds against the United States), and Article 134 which allows federal statutes specific to fraudulent activities to be punished under the UCMJ. Other relevant articles of the UCMJ include: Article 77 (Principals), Article 78 (Accessory after the fact), Article 80 (Attempts), Article 81 (Conspiracy), Article 83 (Fraudulent enlistment, appointment or separation), Article 103 (Captured or abandoned property), Article 107 (False official statements), Article 121 (larceny), Article 123 (Forgery), Article 123a ("bad check" offenses), and Article 134 (bribery and graft).

b. Regulations and orders.

(1) SECNAVINST 5430.107 establishes NCIS' authority and responsibility to investigate all major crimes pertaining to Department of Navy (DON) personnel and assets, including fraud.

(2) DOD Instruction 5505.2, Criminal Investigations of Fraud Offenses, sets forth policies, responsibilities, and procedures for DOD Criminal Investigative Organizations (DCIO) during the conduct of fraud investigations under both U.S. Code and the UCMJ. In accordance with this instruction, the Defense Criminal Investigative Service (DCIS) has primary jurisdiction over all fraud investigations pertaining to contracts awarded to “Top 100” contractors or subcontractors (this list is maintained by DOD/IG and is based on the dollar value of contracts with DOD), the Defense Reutilization and Marketing Service (DRMS) within the Continental United States (CONUS), fraud committed by healthcare providers associated with TRICARE, and kickbacks or bribery involving civilian employees of the Office of the Secretary of Defense (OSD). One item of note, fraud investigations conducted by DCIOs are not restricted under 18 USC 1385, The Posse Comitatus Act. As such, there is more leeway in investigating civilian suspects than normally found in a criminal investigation.

(3) NCIS has primary jurisdiction on contract and procurement actions awarded by the DON regardless of what organization administers the contract (except those circumstances mentioned in the previous paragraph). SECNAVINST 5430.92B, Assignment of Responsibilities to Counteract Acquisition Fraud, Waste, and Related Improprieties Within the Department of the Navy, dated 30 Dec 05, established the Acquisition Integrity Office within the DON Office of General Counsel (OGC) as the central point of coordination for all fraud investigations pertaining to the DON. As set forth in this instruction, the DON Assistant General Counsel/Acquisition Integrity (AGC/AI) manages and directs all acquisition fraud matters within the DON, to include NCIS investigations. Acquisition fraud investigations are defined as those within the following categories:

4A (Antitrust), 4C (Conflict of interest), 4D (Defective Pricing), 4G (General Procurement), 4H (Bribery), 4L (Subcontractor Kickbacks), 4M (Cost Mischarging), 4N (Environmental Crime), 4P (Product Substitution), and 4X (Special Inquiry). NCIS will notify the AGC/AI in a timely manner when an investigation of acquisition fraud is initiated and provide updates regarding significant developments. Based on NCIS investigative efforts and in coordination with NCIS, AIO personnel may initiate legal and/or administrative action against the subject of the NCIS investigation to ensure all legal and administrative avenues are being pursued. The AIO actions will not interfere with the NCIS investigation. Coordination with AIO is not a substitute for coordination with command or the appropriate U.S. Attorneys Office.

(a) NCIS maintains a senior representative at AIO who serves as a liaison point between NCIS and the DON leadership on all issues pertaining to acquisition fraud as defined in the previous paragraph. Part of these duties includes providing copies of all Reports of Investigation (ROI) pertaining to acquisition fraud to the AIO legal staff for their review. As such, all ROIs pertaining to acquisition fraud should include the following in the information section of the distribution line "NCIS AIO Representative". The NCIS representative will in turn brief the appropriate AIO personnel and inform the case agent of this action. Case agents will document this brief in the first subsequent ROI.

(4) DOD Directive 5525.7, Implementation of the Memorandum of Understanding between the Department of Justice and Department of Defense Relating to the Investigation and Prosecution of Certain Crimes, implements an MOU between DOD and the Department of Justice (DOJ) regarding fraud investigations and delineates areas of responsibility for the investigation and prosecution of offenses over which the two departments have concurrent jurisdiction.

(5) DOD 5500.7-R, the Joint Ethics Regulation (JER), details standards of conduct for all personnel, active duty and civilian, associated with the DOD. While this regulation is administrative in nature, it can be used to the benefit of a criminal investigator to gain leverage over or the cooperation of personnel involved in or aware of unethical activities.

(6) The Federal Acquisition Regulations (FAR) and the DOD FAR Supplemental (DFARS) are administrative regulations that set forth guidelines controlling the solicitation, acceptance, and implementation of any contract associated with DON entities. While violations of these administrative regulations by themselves do not constitute criminal conduct, they may be indicative of a bigger problem that warrants further investigation.

c. Within the USC are statutes on fraud that apply to all persons subject to Federal court jurisdiction who commit frauds against the U.S., whether they are in the military service or not. Persons not subject to the UCMJ who commit frauds against the government during the conduct of business with the military are subject to Federal law as applied through the Federal courts. Persons subject to the UCMJ are subject to these laws either as applied through the Federal courts or through court-martial. As applied through Article 134 of the UCMJ, the Federal statutes generally apply without regard to geographical limitations.

24-4.3. The status of an individual suspected of a fraud against the U.S., the offense, and the geographical location of the offense must be considered in determining whether NCIS, DCIS, or the

Federal Bureau of Investigation (FBI) has the predominant authority to conduct an investigation.

a. Matters involving civilian suspects should always be coordinated with the U. S. Attorney's office early in the investigation. NCIS can conduct and/or participate jointly in an investigation if the Navy has a legitimate interest in the investigation. If the appropriate government agency declines to investigate, NCIS will investigate suspected frauds, as long as a continuing DON interest exists, regardless of who may be suspected. For example, in a situation where the FBI declines to investigate a matter, the NCIS should continue the investigation to satisfy DON interest. If information is subsequently surfaced to indicate that the DOJ may wish to consider rendering a prosecutive opinion, the NCIS component controlling the investigation should contact the nearest U. S. Attorney for a prosecutive decision. In overseas environments where a U.S. civilian is the subject of an NCIS fraud investigation, a determination for prosecutive venue will be made via the Military Extraterritorial Jurisdiction Act of 2000 (MEJA) by the DOJ, Washington, D.C. This will be accomplished through a request via Report of Investigation (ROI) from the NCIS component to NCISHQ (Code 23A) under the guidelines of DOD Instruction 5525.11.

b. Frauds committed by persons subject to the UCMJ will be investigated by NCIS to determine the nature and extent of the crime.

c. In accordance with DOD Directive 5525.7, NCIS must refer all "significant" allegations of bribery and conflict of interest involving DOD personnel to the FBI. As defined by this directive, “significant” allegation includes any of the following circumstances: allegations involving present, retired, or former General or Flag Officers and current or former members of the Senior Executive Service (SES). Other factors that impact on the need to refer investigations to the FBI include the sensitivity of the DOD program impacted, the monetary value of the alleged bribe, and the number of DOD personnel involved. These factors are not clearly defined in the MOU and must be considered on a case-by-case basis.

d. In accordance with SECNAVINST 5800.12B, Investigation of Allegations Against Senior Officials of the Department of the Navy, dated 12 Oct 05, NCIS must also notify the DOD Inspector General of any allegations of the criminal activity by any of the following personnel: present, retired, or former General or Flag Officers or those selected to become General or Flag Officers, any current or former members of the Senior Level (SL) or Scientific and Professional (ST) , and current or former presidential appointees.

e. Unless NCIS is promptly advised otherwise by the FBI, the investigation by NCIS will be continued. Upon notification by the FBI that they have assumed investigative jurisdiction, NCIS will continue the investigation concurrently with the FBI. Whenever possible, the decision with respect to jurisdiction in a given case should be made at the local level. If agreement cannot be reached at that level, the matter should be referred to NCISHQ for resolution. If military authorities believe that the crime involves special factors relating to the administration and discipline of the Armed Forces that would justify exclusive investigation by NCIS for the purpose of court-martial, the NCIS component shall promptly advise the FBI. Investigation in such a case may be undertaken by NCIS if the DOJ agrees.

f. Allegations of bribery and conflict of interest that result from events that occurred outside

the United States, its territories, and possessions, do not need to be referred to the FBI.

g. In a country where U. S. Armed Forces are present as guests, investigation by NCIS of frauds committed against the U.S. by local nationals are normally conducted according to the agreements between the U.S. and the host country.

24-4.4. Liaison With Other Agencies. In order to obtain required information in procurement fraud investigations, it is often necessary to effect liaison with certain government agencies and activities. The following agencies may provide assistance:

a. Federal Bureau of Investigation (FBI). Investigation of fraud, bribery, and other crimes involving government contracts is within the investigative jurisdiction of the FBI. Close coordination and cooperation between NCIS and the FBI at the local and occasionally the national level is essential. Concurrent jurisdiction often exists between the DOJ and the DOD. As mentioned in Paragraph 24-4.2.b.(4), DOD Directive 5525.7 (Implementation of the Memorandum of Understanding Between the Department of Justice and the Department of Defense) delineates the area of responsibility of each, priorities in the case of concurrent jurisdiction, and the procedures to be followed. Normally, where there appears to be a prima facie case, the appropriate U.S. Attorney will assume prosecutive interest and jurisdiction and the FBI will undertake any further investigation in conjunction with NCIS. A declination by the FBI to actively investigate a specific violation of federal law is a release for the NCIS to continue the investigation and present the matter to the appropriate U.S. Attorney for prosecution.

b. Defense Criminal Investigative Service (DCIS). The DCIS has interest in various matters pertaining to fraud with the DOD. Specifics are set forth in DOD Instruction 5505.2.

c. Internal Revenue Service (IRS). The IRS has interest in violation of federal tax laws and in any income resulting from unlawful procurement relationships which may not have been reported.

d. General Services Administration (GSA). The GSA has interest in government procurement, construction, and supply contracts. This agency may provide information regarding suspect firms or individuals.

e. U.S. Army Criminal Investigation Command (CID). The CID may provide information concerning the involvement of suspected firms or individuals in Department of the Army procurement actions.

f. U.S. Air Force Office of Special Investigations (OSI). The OSI may provide information concerning similar involvement of suspected firms or individuals in Department of the Air Force procurement actions.

g. Defense Contract Audit Agency (DCAA). The DCAA is a function of the Undersecretary of Defense (Comptroller) and conducts administrative audits throughout the DOD. Discovery of indications of fraud, collusion, or wrongdoing during the course of an audit is reported pursuant to departmental regulations and procedures. However, auditor's working papers may, at a later date, provide information pertinent to a particular investigation, which at the time of the audit, did not

appear significant. Attempts by the contractor to insert or "hide" non-applicable costs are often detected and not accepted by auditors, but if corrected and not contested by the contractor, these irregularities may not be pursued. A history of such practice by a particular contractor may be pertinent and may be developed in coordination with the auditors concerned. Continuing liaison with DCAA is a necessary element in maintaining surveillance to detect or deter procurement fraud. In specific cases, and on proper request, auditors from the DCAA may be detailed to conduct special audits and inspections of records at contractor facilities when fraud is suspected.

h. Defense Contract Management Agency (DCMA). The DCMA is an administrative arm of the Defense Logistics Agency (DLA). DCMA manages contracts throughout the DOD and conducts quality control and physical inspections of products received. Contract records are maintained by DCMA which operates through Regional District Offices (DCMAS) and local offices (DCMO) at the site of major contracts. The local or district office may be consulted by the agent for review of contracts, changes thereto, and for referral to other agencies which may be helpful in acquiring a complete picture of an individual contract and the contractor's performance. NCIS Special Agents can obtain records of contracts, invoices, etc through DCMA without the use of a subpoena.

i. Naval Audit Service (NAVAUDSVC). The NAVAUDSVC is charged with the responsibility for the audit of Naval activities and installations. When a NCIS component determines the need for audit assistance from NAVAUDSVC, the agent should forward a written request to the Auditor-in-Charge of the NAVAUDSVC, defining the particular needs of the requesting NCIS office. The request for assistance should then be reported in the next ROI for the investigation in question with a copy of the letter of request as an exhibit to the report.

j. Military Procurement Agencies. A determination should be made as to whether suspect firms or individuals have (or have had) contractual relationships with any of the service procurement agencies. Examination of the records of these agencies, after proper coordination, should proceed to the extent necessary to determine whether there exists a pattern of conduct relevant to the allegations under investigation or evidence of additional offenses. Depending on the dollar amounts of contracts concerned, records of awards to a specific contractor may be found by querying a DOD database of all DD350 (Individual Contracting Action Report) forms on file for that company. This database can be accessed at the local level or via a request to Code 23. Also the Navy Air Force Interface (NAFI) maintains a database of all contracts, modifications, delivery orders, etc utilized within DOD. This database, the Electronic Document Access database (EDA), is a secure web-based system that provides storage and retrieval of acquisition-related documents used by multiple DOD agencies and commercial vendors. EDA provides online access to business documents such as contracts, contract modifications, personal property and freight government bills of lading (GBLs), vouchers, Contract Deficiency Reports (1716s), summaries of Voucher Line Data (110 reports), Material Acceptance Payable reports (MAAPRS) and Army direct vendor deliveries (DVDs). The system architecture includes the communication, data translation and conversion, and infrastructure components necessary to support the application.

k. General Accounting Office (GAO). GAO personnel may be contacted for data obtained during GAO audits or for assistance of a technical nature in the review of certain records and

transactions.

24-5. ANTITRUST (SUBCATEGORY 4A).

24-5.1. Antitrust violations are contrary to U.S. Government policies for free and open competition and circumvent government efforts in affecting competitive contracting methods. The offenses associated with antitrust violations invariably result in increased costs to government, corrode the free enterprise system, and destroy public confidence in the national economy. The Sherman Anti-Trust Act of 1890 (15 USC 1) established conspiracy in restraint of trade or commerce as a felony. The element of conspiracy is necessary in antitrust violations because not only is it important to show that an agreement was reached pertaining to the restraint of trade, but an overt act in furtherance of the agreement must also be committed. A conspiracy in an antitrust violation can produce damage to the federal acquisition process and prove catastrophic in an atmosphere of national emergency. The elements of a criminal offense in an antitrust violation are the formulation of any illicit agreement on the part of two or more competitive vendors and their resultant restraint of interstate trade or commerce. Specifically, it must be ascertained that the conspirators agreed, formally or otherwise, to fix or stabilize prices or to allocate customers, territories or markets; further, that the conspiracy affected products, services, or funds traveling in the flow of interstate commerce. The term "interstate commerce" is interpreted as any business activity that may be conducted in the United States. The Act also applies to intrastate commerce, business activities conducted within a specific state. The Antitrust Division, United States DOJ has primary prosecutive jurisdiction in all Federal antitrust violations. Its field offices are located in Atlanta, Chicago, Cleveland, Dallas, Philadelphia, New York City, and San Francisco.

24-5.2. Antitrust violations are as many and as varied as their perpetrators, and have been discovered in conjunction with numerous commodities and services contracted for by the DOD. Such violations include, but are not limited to:

a. Bid Suppression, also known as Bid Limiting. Whenever one or more vendors collude with a competitor to refrain intentionally from submitting bids to the government so the contract must be awarded to a specific firm, Bid Suppression occurs. This is a violation of both 15 USC 1, Monopolies and Combinations in restraint of trade, and 18 USC 371, conspiracy to commit any offense against the United States or to defraud the United States. Vendors may also submit fabricated bid protests to compromise the government's selection of a supplier, claiming that the technical evaluation of a proposal was not properly conducted, that the low bidder was not responsible and therefore not qualified to perform the work, or that the bidder who was awarded the contract was not responsive to the invitation for bids or proposals. Such fabrication is within the scope of Fraud and False Statements and is governed by 18 USC 1001. Another example of Bid Suppression is an active attempt on the part of a vendor to influence suppliers and subcontractors not to deal with non-conspiring vendors, another violation of 18 USC 371, in that such activity, especially as part of a conspiracy, defrauds the United States by negating a spirit of free enterprise among eligible contractors. In addition, such influence, if effective, can increase government costs significantly and may also result in both increased administrative lead-time and longer production and delivery schedules.

b. Complementary Bidding, also known as Shadow Bidding or Protective Bidding. Vendors

who intentionally submit bids that are either too high in cost or contain specific terms that are unacceptable to the government and in effect cause a government contract to be awarded to another bidder, are participating in Complementary Bidding. The objective of this scheme is to create the illusion of submitting a bona fide offer while in reality pricing one's proposal beyond fair and reasonable terms in the hopes that a conspiring vendor's lower bid or more acceptable contract terms will win government favor. The firm submitting the unrealistic bid may pad its proposal with increased supplier's costs, inflated subcontractor's costs, fictitious tooling, overhead, shipment or packaging costs or unacceptable delivery schedules. This is a combination of conspiracy as governed by 18 USC 371 and False Statements as contained in 18 USC 1001.

c. Price Fixing. This scheme takes many guises. One example can be viewed as a collusive agreement on the part of competitive vendors to adhere to published price lists. Conspirators may also agree to identical increases in costs, identical discount terms, unadvertised prices, or to policies maintaining specified price differentials based on the quantity of contracts. The principal advantage of price fixing is that by adhering to maximum or minimum price schedules in selected commodities or services, conspiring vendors cause non-conspiring vendors to sell in accordance with their own judgment. Price Fixing is designed to eliminate competition within the specified industry and to retain the market for those vendors who have agreed among themselves to control costs. Price fixing is frequently evidenced in the scheme of Collusive Bidding, whereby an anti-competitive climate is created through one or more of the following strategies:

d. Identical bids may be submitted by two or more contractors.

(1) Price increases occur simultaneously and in identical increments.

(2) Bids may be decreased by conspiring vendors in the event of an offer from a nonconspiring vendor.

(3) Vendors insist that they are adhering to "industry-wide" or "market-wide" prices or are offering their products or services at "association price schedules."

(4) Specific contractors either consistently bid against each other or invariably refrain from bidding against each other.

(5) Bids are withheld without apparent reason by vendors who are fully qualified and equipped to perform the work.

The above examples violate not only 15 USC 1 and 18 USC 371, but are also in violation of FAR 3.103, Independent Pricing. FAR requirements specify that a certificate stating the prices were determined independently without any agreement to restrict competition must be inserted in solicitations for a firm-fixed-price contract (with or without economic price adjustment), with some exceptions. The largest exception is where small purchases are made which do not exceed $25,000 (FAR 3.103-1 and 13.000).

e. Bid Rotation, also known as "Teahousing" or "Brother-in-Law Bidding." In this scheme, competitive vendors conspire in taking turns as low bidder. This is a common occurrence and

difficult to prove because of the ease of collusion involved and the many simple methods of keeping the scheme clandestine. While the practice is socially acceptable in some cultures, it is not considered ethical in United States government contracting because it compromises genuine competition within the acquisition process and is clearly an example of collusion among vendors. Bid Rotation is a direct violation of 18 USC 371 and 15 USC 1. Since a vendor in collusion with other competitors knows it is his turn to be the low bidder, the quality of the product or service may be well below standard. Further, no sincere attempt is made at keeping costs down, since the other conspirators' bids will be high. The end result is frequently increased cost to government, not only in terms of dollars but in substandard contractor performance.

24-5.3. A vendor may become involved in antitrust violations for numerous reasons, among them:

a. A false sense of job security, in that participation in collusion with other firms will always provide a share of government contracts, as in Bid Rotation.

b. A sense of obligation to co-conspirators for favors, bribes, loans, or business leads.

c. A false sense of belonging to an elite circle of businessmen who protect their mutual interests by undermining the competition.

d. Lack of personal integrity, self-confidence, or motivation to act independently.

24-5.4. The perceived advantages of conspiring vendors are far outweighed by the ultimate consequences that are:

a. Increased costs to government through the needless expenditure of funds and man-hours because contract costs are usually high in an antitrust climate.

b. Substandard contractor performance, directly translatable into a decreased mission posture for government agencies.

c. Legal ramifications for conspirators, including fines, incarcerations, suspensions, and debarment.

d. Degradation of the free enterprise system, in that bona fide contractors' efforts are compromised.

e. Permanent damage to a conspirator's reputation, business integrity, and capacity for public trust.

24-6. CREDIT CARD FRAUD (SUBCATEGORY 4B).

24-6.1. When an individual or organization obtains or attempts to obtain a product, service, or anything of value by means of an access device with the intent to defraud, a criminal act takes place. The term "access device" is defined by 18 USC 1029 as "any card, plate, code, account number, or other means of account access that can be used alone or in conjunction with another access device to

obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument)." The term "counterfeit access device" means "any access device that is counterfeit, fictitious, altered or forged, or an identifiable component of an access device or a counterfeit access device." The term "unauthorized access device" means "any access device that is lost, stolen, expired, revoked, cancelled, or obtained with intent to defraud."

24-6.2. There are numerous methods that are commonly used to perpetrate credit card fraud. The following list is not all inclusive but rather is intended to highlight some common schemes:

a. Altered credit cards. These are credit cards that were manufactured by an authorized issuer, but were subsequently lost or stolen and then re-embossed, re-fabricated, or otherwise modified to reflect a different name, account number, expiration date or signature.

b. Counterfeit credit cards. These are access devices that have been printed, embossed, or encoded in imitation of valid devices, but are not authorized by a bona fide manufacturer. Embossing machines to produce counterfeit cards can be readily purchased or stolen.

c. Substitute or "white plastic" cards. A blank piece of plastic, credit card size, may be embossed with a valid cardholder's name, account number and expiration date. This device is then imprinted on a sales draft and presented for payment as though it were a completed transaction of a valid payment device.

d. Telemarketing or Internet Fraud. A person may contact a card holder via telephone or e-mail advise the card holder that he wishes to sell a particular item or present a gift. All that is necessary is for the cardholder to tell the caller his name, address, and credit card number. The same scheme may be applied through mail order.

e. Obtaining valid account numbers. This can be accomplished by obtaining credit card receipts that were used in valid transactions and discarded by merchants or customers. It can also be done by simply copying or memorizing a cardholder's account number when standing behind him in line when he makes a purchase or by borrowing the card.

f. False Billing. This is the duplicating of credit card receipts. After acquiring a credit card number through an ordinary transaction, a merchant may process other actions that do not actually take place.

g. "Bust-Out" Operations. A business may be created for the sole purpose of submitting fraudulent charges. Unscrupulous persons may form a corporation under alias names, open a bank account, and obtain authorization to accept credit cards. They then submit an exorbitant amount of credit card claims in a short while and dissolve the business.

24-6.3. Criminal penalties for such offenses are prescribed by 18 USC 1029, Fraud and Related Activity in Connection with Access Devices. The statute specifies that the United States Secret Service (USSS) shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section. Credit card fraud is also addressed by 15 USC 1644,

Fraudulent Use of Credit Cards. Violations governed by that statute are:

a. Unlawful use, attempt, or conspiracy to unlawfully use a card in a transaction affecting interstate or foreign commerce.

b. Transporting, attempting, or conspiring to unlawfully transport a card in interstate commerce.

c. Unlawful use of interstate commerce to transport or sell a card.

d. Receipt or concealment of goods obtained by unlawful use of a card.

e. Receipt or concealment of tickets for interstate or foreign transportation obtained by the unlawful use of a card.

f. Furnishing of money through unlawful use of a card.

24-6.4. Telephone Calling Cards. In general, NCIS will investigate the fraudulent use of telephone calling cards where the government is not the victim only if a felony has been committed. The monetary threshold used to determine whether or not to initiate an investigation will be determined by local field offices in coordination with base investigators and prosecutorial authorities.

a. Applicable statutes include:

(1) Under Article 121 (larceny), UCMJ, at least one single incident must exceed $500 in order to constitute a major offense.

(2) Under 18 USC 1029 (fraud and related activities in connection with access devices), chargeable under Article 134, UCMJ, situations where an aggregate of $1,000 worth of fraud in a 1-year period constitute a major offense.

(3) Under 18 USC 1343 (fraud by wire), chargeable under Article 134, UCMJ, certain fraudulently made telephone calls in "interstate or foreign commerce" are major offenses.

b. Matters not meeting the major-offense criteria (more than 1 year imprisonment authorized in the Manual for Courts-Martial as punishment) should not be investigated by NCIS. Further, NCIS should decline to investigate those cases where the loss is over $1,000 where there are an extremely large number of culprits who each made small value calls. An example is when a telephone calling card number is passed around an entire ship's company. Limited assistance may be provided on a case-by-case basis where command resources are lacking and where judicial action is contemplated. In non-major-offense cases where the telephone company solicits NCIS assistance, efforts should be made to facilitate the requests, without expending substantive NCIS resources; examples would include liaison with command and providing the full identification of DON suspects or witnesses. NCIS should not serve in a bill- collecting capacity for commands and commercial firms. Matters not investigated by NCIS should be documented by ROI (INFO) so that the culprit(s) can be entered into the Defense Central Index of Investigations (DCII).

c. If a service-connected person commits a related offense outside an area of primary government jurisdiction and the government is not the victim, investigative jurisdiction rests with other investigative agencies, i.e., local police or company investigators. Absent significant government interest, NCIS will normally not investigate the latter cases except as follows. NCIS may conduct reciprocal investigations upon request by civilian police agencies, commercial telephone company investigators, or other investigative agencies when:

(1) Good order, discipline, or community reputation of the service might be significantly affected by the crime(s);

(2) A non-government entity is the sole victim and the other investigative agency has no other investigative recourse (e.g., the suspect(s) or pertinent records are physically out of reach of the investigative agency);

(3) An NCIS declination of reciprocal assistance would significantly impair NCIS liaison with the other investigative agency.

d. Discretion must be exercised to preclude expenditure of NCIS investigative effort where NCIS has no jurisdiction or where appropriate government interest does not exist.

24-7. CONFLICT OF INTEREST/STANDARDS OF CONDUCT (SUBCATEGORY 4C).

24-7.1. The Joint Ethics Regulation (JER) provides that DON personnel will not accept any favor, gratuity, or entertainment that might affect, or might reasonably be interpreted as affecting, or give the appearance of affecting the objectivity and impartiality of such personnel in serving the Government. Favors, gratuities, or entertainment bestowed upon members of the immediate families of DON personnel are viewed in the same light as those bestowed upon DON personnel. Acceptance of entertainment, gifts, or favors (no matter how innocently tendered or received) from those who have or seek business dealings with the DOD may be a source of embarrassment to the Department and to the personnel involved, may affect the objective judgment of the recipient, may impair public confidence in the integrity of business relations between the Department and industry, and must be discouraged. Violations of the JER are punishable under Article 92, UCMJ and administrative action can be taken against civilian DON employees.

24-7.2. As a result of enactment by Congress of 18 USC 201, which broadens the bribery statute both as to acts prohibited and personnel covered, some acts formerly classified as gratuities under the JER now constitute bribery. For a discussion of when the giving of a thing of value is or may be bribery and when it is or may be a gratuity, refer to subcategory 4H for guidance. Most investigations of gratuities involve the giving and receiving, rather than only a solicitation or an offer. Thus, both DON and non-DON personnel are involved. The prohibition regarding the acceptance of gratuities extends to all DON personnel and members of their immediate families. However, it especially concerns procurement personnel and those engaged in activities related to procurement. This includes not only buyers and contracting officers, but personnel who prepare requirements, administrative contracting officers, inspectors, and others who deal with contractors both before and after award. Usually, acceptance of gratuities is revealed through complaints of

DON or contractor personnel. The acceptance of gratuities may include the receipt of gifts, the use of a hotel room at no cost, or the acceptance of entertainment including lunch or dinner with a contractor. It is especially important to obtain full and complete details from the complainant. Corroborative evidence documenting the source of the gratuities, including the nature, purpose, and cost involved should be obtained. If the DON employee was on TDY, travel claims may establish that he was in the area at the time of the entertainment.

24-7.3. If a DON employee has received gratuities, the possibility that he may be returning favors should not be overlooked. Quite often, acceptance of gratuities is coupled with charges of favoritism. The position of the DON employee should be ascertained to determine whether the employee would be able to help the contractor. Any dealings the DON employee had with the contractor should be determined through records review and by interview of supervisors or others. The DON employee should be interrogated and a signed sworn statement solicited. The contractor or the representative who gave the gratuity should be interviewed to determine why the gratuity was furnished, whether the cost was charged to a DON contract or carried as a general business expense, and whether the contractor is aware of the DON prohibition against accepting gratuities.

24-7.4. Legislation pertaining to conflicts of interest, in effect since 1963, broadened both the conduct prohibited and the personnel covered, and created a class of "special government employees" to whom special conflict of interest rules applied. The legislation applicable to the DON is contained in 18 USC 203 and 205-09.

24-7.5. 18 USC 203 broadens the prohibitions of former Section 281. It expands the class of persons affected the category of proceeding to which the disqualification applies, extends the penalty to the giving as well as the receiving of compensation, and applies a rule to special government employees which is less restrictive than that applied to regular government employees. It corrects the failure of former Section 281 to prohibit preemployment receipt or agreement to receive, or post-employment receipt of compensation with respect to service to be rendered or actually rendered during the period of government employment.

24-7.6. 18 USC 205 allows the employee to aid or assist in the prosecution of a claim against the government provided he receives no compensation for services. If, however, the employee receives a gratuity, share, or interest in any claim in consideration for his assistance in the prosecution of the claim, the employee comes within the prohibition of the statue. If he acts as an agent or attorney for prosecuting a claim against the government, as opposed to merely aiding or assisting in the prosecution, he is within the scope of the statute regardless of whether he receives any compensation for services. By not modifying the term "agent" in Section 205(2) with the phrase "for prosecution," the scope of Section 205(2) is extremely broad, covering nearly every conceivable activity which an employee may perform in a representative capacity for another before the designated government agencies. The status of retired officers was left unchanged by the new statutes. Sections 281 and 283, insofar as they apply to retired officers, were not repealed.

24-7.7. 18 USC 207 replaces the former 18 USC 284 and deals with post-employment conflict of interest. It was amended in 1978 as part of the "Ethics in Government Act of 1978" (Public Law 95-521) and further amended in 1979 (Public Law 96-28). Section 207(a) places a lifetime bar on a former government employee acting as agent or attorney for anyone in connection with any

particular matter before the government in which the U.S. has a direct and substantial interest and in which the former employee participated personally and substantially as a government employee. Section 207(b) places a 2-year bar on a former senior Government employee from aiding or assisting in the representation of another person in connection with an appearance before the government only when the former employee is personally present at the appearance and when the particular matter in issue is one in which he personally and substantially participated as an employee of the government. Section 207(b) also imposes a 1-year ban which bars a former senior employee from attempting to influence his former agency on a matter that is pending before, or of substantial interest to, the agency for one year after he ceases being a senior employee. The 1-year bar applies even if the senior employee had no prior involvement in the matter. This prohibition reaches attempts to influence not only "particular matters" but also general rule making.

a. The 1-year ban, as amended, excludes from its prohibitions former senior employees who have become elected state officials, full time employees of state and local governments, employees of accredited institutions of higher learning or employees of hospitals or medical research organizations granted tax exemption by the Internal Revenue Service when acting on behalf of these organizations. The amendments also permit the Director of the Office of Government Ethics to further limit the application of the 1-year ban so that in given cases former senior employees will only be prohibited from contacting specific offices within their former departments or agencies as opposed to being barred from contact with the entire department.

b. The 1- and 2- year bans noted above only apply to "senior employees" and that term means former employees of the following categories:

(1) Executive Scheduled Employees,

(2) Officers of the Grade of O-9 and O-10, and

(3) The following personnel when designated by the Director of the Office of Government Ethics as serving in positions that involve significant decision making or supervisory authority:

(a) Employees paid at the basic rate GS-l5 and above,

(b) Members of the Senior Executive Service, and

(c) Officers of the Grade of O-8 and O-7.

24-7.8. 18 USC 208(a) replaces former 18 USC 434, which disqualified government officials who have an interest in the profits or contracts of a business entity from the transaction of business with such entity. Section 208(a) abandons the transaction of business concept and disqualifies the employee from participating personally and substantially on behalf of the Government in a matter, even though his participation does not involve the transaction of business. Section 208(a) goes beyond former Section 434 in that it disqualifies an employee from participating in a matter in which not only he, but, to his knowledge, his spouse, minor child, partner, organization in which he is serving as officer, director, trustee, partner, or employee, or any person or organization with whom

he is negotiating or has any arrangement concerning prospective employment, has a financial interest. This would cover nonprofit organizations such as universities, foundations, and nonprofit research entities as well as business organizations.

24-7.9. Gambling. Because the JER prohibits gambling, betting, and lotteries by DOD personnel on government owned or controlled property (with some exceptions), subcategory 4C will be used to document such activity. In addition to this being an Article 92, UCMJ, violation for military members, various state and federal violations may pertain. For civilian suspects, NCIS policy requires that a major-offense violation be suspected or alleged before NCIS resources will be expended in an investigation.

24-8. DEFECTIVE PRICING (SUBCATEGORY 4D).

24-8.1. Defective pricing occurs whenever a defense contractor knowingly overprices negotiated government contract prices by quoting performance costs higher than those of actual expenditures or fails to reveal all costs associated with a contract. Performance costs include, but are not limited to: design costs; engineering; prototypes; overhead; labor costs; manufacturing costs; subcontracting; facilities; material costs; tooling; packing, packaging and shipping. Costs of the products or services purchased by DOD through the free enterprise system will naturally vary. The most significant contributing factors in price differences are the varying labor rates throughout the country, the fluctuating costs of raw materials and the ceiling on what the market will bear. A primary issue in determining Defective Pricing for commodities is the application of "fair and reasonable" criteria as determined by price analysts within the buying activities. The "fair and reasonable" cost of a commodity is reckoned mainly by the items past price history, current production costs, varying labor scales, and inflation rates.

24-8.2. Both 18 USC 287 (Fraudulent Claims) and 18 USC 1001 (False Statements), apply to the evaluation of vendors' proposals, in that one or both would be violated by the unscrupulous padding of costs on the part of the supplier.

24-8.3. The Truth in Negotiations Act (Public Law 87-653 or 10 USC 2306A) requires that cost or pricing data be obtained in specific contracting situations and only in situations of acquisition by negotiation. The Act also provides exceptions to that requirement. Cost or Pricing Data should never be required unless the contracting officer concludes that none of the exceptions to the cost or pricing data requirement are appropriate. When no exception is appropriate, in the following circumstances, cost or pricing data would normally be obtained:

a. The award of any negotiated contract (except for those actions not defined such as letter contracts) expected to exceed $500,000.

b. The award of a subcontract at any tier, if the contractor and each higher-tier subcontractor have been required to furnish cost or pricing data.

c. The modification of any sealed bid or negotiated contract (whether or not cost or pricing data were initially required). This requirement also applies to subcontracts if the

contractor and each higher-tier subcontractor have been required to furnish cost or pricing data.

24-8.4. Under FAR 15.401, "Cost or Pricing Data" means all facts as of the time of price agreement that prudent buyers and sellers would reasonably expect to affect price negotiations significantly; are factual, not judgmental, and are therefore verifiable; include the data that form the basis for the prospective offer or judgment about future cost projections; are more than historical accounting data. They are all the facts that can be reasonably expected to contribute to the soundness of estimates of future costs and to the validity of determinations of costs already incurred. They include such factors as vendor quotations, nonrecurring costs, and information on changes in production methods and in production or purchasing volume.

a. Exceptions.

(1) Adequate price competition;

(2) Commercial item;

(3) Price set by law or regulation; and

(4) Waiver exception.

24-8.5. Mistakes in bids are managed in accordance with FAR 14.406, which contains all government provisions for clerical errors, bid verifications, and records determinations.

24-8.6. A contract finalized within the parameters of the Truth in Negotiation Act contains a price-reduction clause in the event of overpricing because of inaccurate, incomplete or non-current data submission by the contractor. Government compensation for overpayment to a contractor who knowingly provided inaccurate cost data is governed by Public Law 99-661, Defense Authorization Act. This statute assesses such a contractor with a penalty amount equivalent to the contract overpayment, plus interest, until final restitution is made.

24-8.7. Defective Pricing can be a high-cost fraud offense, either because of numerous inflated small purchase contracts or because of the high dollar cost involved in large acquisitions. Several factors indicative of defective pricing are:

a. A large number of contract line items on a single purchase, where the cost of several, although inordinately high, appear acceptable as part of the order.

b. Contractual actions for obsolete or esoteric components that are long out of manufacture and have no recent price history.

c. Production items requiring special tooling, materials or facilities, where costs are not readily determinable or where market costs have not been established.

d. Expedited first-run manufacture items, where production costs are estimated on a contingency basis.

e. A contractor's desire for exorbitant profits or lack of discrimination in determining reasonably priced materials and subcontractor.

24-9. PAY AND ALLOWANCE (CATEGORY 4E).

24-9.1. These investigations are conducted upon specific allegations of possible fraud or other irregularities in connection with the disbursement of DON funds. The DON has primary interest in these investigations to ensure that its operations in regard to disbursement of funds are proper. Pay and Allowance investigations are conducted to develop information concerning the validity of payments made by Navy and Marine Corps accounting and finance officers, with the purpose of effecting recoupment of monies erroneously paid.

24-9.2. The following glossary of terminology applicable to this case category will be useful to the special agent:

a. Defense Finance and Accounting Service (DFAS). The central repository for all finance records and the disbursement center for such items as allotments and retirement pay is located in Cleveland, OH.

b. Allotment. That portion of the pay and allowance of a member that he authorizes to be paid to an allottee in a manner prescribed by law.

c. Allotment Authorization. An accounting and finance document executed by service members to initiate, terminate, or change an allotment.

d. Allowances. Funds paid to service members to defray expenses incurred in connection with the performance of official duties. Examples are travel allowance, clothing allowance, Basic Allowance for Housing (BAH), and Basic Allowance for Subsistence (BAS), and Overseas Housing Allowance (OHA).

e. Dependency Certificate (DD Form 137). A form executed by a service member to establish a claim for BAH based on dependency. This form must be executed periodically and at the time dependency changes occur.

f. Entitlement. The basic regulation, law, or order upon which claim for payment is based.

g. Joint Travel Regulation (JTR). The JTR is the official regulation governing the travel of service members and their dependents.

h. Military Pay Order (DD Form 114). An accounting and finance document directing changes in a member's pay account authorizing a credit to or deduction from a service member's pay. This is prepared in the service member's unit personnel section.

i. Notice of Exception (NOE). A document issued by the General Accounting Office (GAO) questioning the legality of a particular payment.

j. Parents' Dependency Affidavit (DD Form 137-3). A form executed annually by secondary dependents indicating their financial position to qualify for receipt of an allotment.

k. Pay. Money earned for services rendered. Examples are basic pay, incentive pay for hazardous duty, sea and foreign duty pay.

l. Substantiation. The fulfillment by the service member of requirements of the basic law, regulation, or order, e.g., actual performance of travel.

NOTE: Both entitlement and substantiation are necessary to effect legal payment of a claim.

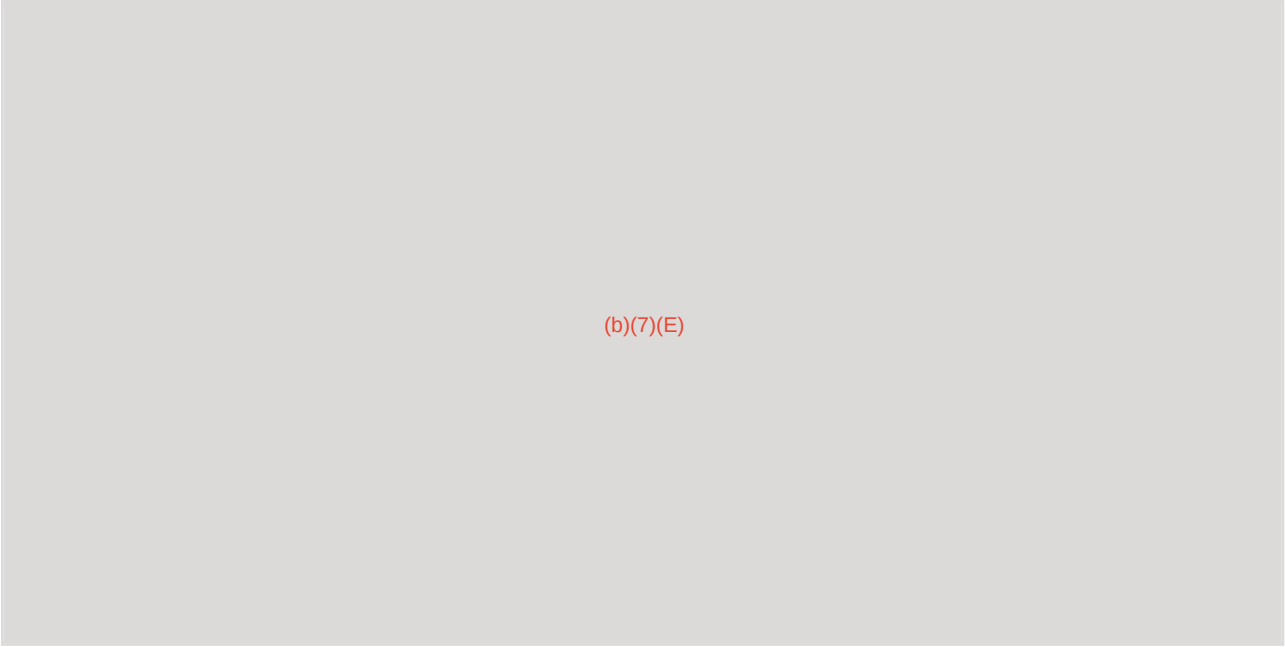
m. Voucher. A written document bearing the signature of the payee and certification that the facts therein concerning the claim are true and correct.

24-9.3. Housing Allowance. An investigation involving Basic Allowance for Housing (BAH) or Overseas Housing Allowance (OHA) is usually predicated upon a specific allegation that the service member is not entitled to the allowance. The status of the service member, whether single or married, determines the factor of entitlement and substantiation to be established in investigations of housing allowances. The various investigations of this type, together with specific requirements as to each and investigative steps recommended to resolve the issues, are set forth below:

a. Members Without Dependents. A service member without dependents is entitled to receive a BAH if he does not occupy government quarters and the allowance is approved by competent authority. The issues to resolve in these investigations are whether the authorization was proper and whether the service member resided in government quarters during the period involved. The following investigative steps should be taken:

(b)(7)(E)

b. Members with Primary Dependents. A service member with primary dependents (lawful wife or unmarried children under 21 years of age) is entitled to BAH if the dependents do not occupy government quarters and he has submitted a DD Form 137 as required. A court order requiring support for minor legitimate or illegitimate children is a proper basis for payment of the BAH, but a court order requiring payment of alimony is not. The problem in these cases is to verify the existence of children or a valid marriage as the basis of payment of the BAH. As to the latter, it is necessary to establish that the previous marriages, if any, of both parties were legally dissolved



c. Members with Secondary Dependents. Full treatment of entitlements and substantiation will be found under subcategory 4I, Dependency Assistance Investigations.

d. Military members may receive BAH when they do not maintain a residence at the permanent duty station while performing on temporary duty. A military member without dependents who is away from his permanent station may occupy government quarters at their temporary duty station without affecting his right to receive BAH to which he was entitled and was receiving at this permanent duty station, as long as the permanent station remains unchanged. Since Variable Housing Allowance (VHA) is merely a supplement to BAH in high housing cost areas within the United States, it follows that a military member, on temporary duty would likewise be entitled to continue receiving such VHA under the same circumstances that he could continue receiving BAH. The duration of the temporary duty is not for consideration. Nor is there any apparent requirement that military members offer proof that they are in fact maintaining their private quarters at the permanent duty station while on temporary duty. However, a military member without dependents who is in a pay grade below E-7 is never entitled to BAH while he is on sea duty. If the military member is a pay grade E-7 or above, he is entitled to BAH only for the first ninety days of sea duty.

24-9.4. Investigations are sometimes initiated by NCIS components when the sole allegation is non-payment of support to dependents. DOD Pay Entitlements Manual (Section 30236) provides guidance to be followed by military commands when a military member refuses to support a dependent. Specifically, "BAH is not payable on behalf of a dependent whom a member refuses to support." When a complaint of non-support or inadequate support is made by a dependent, "The member must provide proof of support." This is considered to be an administrative matter that, absent any unusual circumstances, should be handled by command without NCIS assistance.

24-9.5. Travel Allowances. A service member is entitled to reimbursement for expenses incurred in the performance of travel in connection with official duties and, under certain circumstances, for travel of dependents. All reimbursement of expenditures for travel is claimed by submission of

vouchers.

a. Member's Travel. Normally, investigations concerning a service member's travel involve verification of performance or nonperformance of the travel, dates of travel, and/or utilization of government quarters and messing facilities. Information relative to this travel can usually be developed through examination of military records, such as sign-out registers, morning reports, passenger manifests, and transient billeting records.

b. Dependent's Travel. A service member is entitled to reimbursement for dependent's travel when such travel is performed in connection with permanent change of station (PCS) or assignment to indefinite temporary duty overseas. In each instance, competent orders must be issued and travel must have been performed in accordance with the provisions of the Joint Travel Regulation (JTR). The JTR provides that when dependents travel within the CONUS incident to an assignment overseas, the travel must be performed with the intent to establish a bona fide residence for the duration of the service member's overseas tour, or until the dependent's travel to an overseas location is authorized. Thus, it is necessary to develop evidence relative to bona fide intent to reside. Investigation in dependent travel cases should be directed to developing information concerning the following:

(1) Complete identity of dependent(s).

(2) Location of dependent(s) upon receipt of orders by the service member.

(3) The date of departure and the last address at which the dependent(s) resided prior to departure. This information may be developed through personal interviews and examination of official records.

(4) Intent, where applicable, to establish a bona fide residence at the destination address. Evidence of intent may be established by developing information concerning long-term agreements such as leases and contracts for utility services, as well as representations to others.

(5) Explanation, where applicable, for having the allotment check forwarded to the address on file at the NFC and disposition of the check.

c. "No-receipt" travel claims. NCIS will not investigate travel claims, where the allegation is based solely on "no-receipt" items of cost incurred by the traveler. Such costs where the traveler is not required to submit a receipt are meal expenses, laundry expenses, tips, etc. The Navy Comptroller for Financial Management Systems has determined that an adequate administrative remedy is available to commands in "no-receipt" claims. Unit disbursing officers can disallow a travel claim based upon the disbursing officer's judgment that a claim amount is excessive and the burden falls on the claimant to further support his claim. When the claimant contests the disbursing officer's decision, he must submit proof/substantiation of the claim to the General Accounting Office for consideration.

24-9.6. Subsistence Allowances. Service members may be authorized to receive a Basic Allowance for Subsistence (BAS) under certain circumstances. One of these is permission to ration separately.

The most common basis for authorizing separate rations is the service member's written certification that there is intention for the member to live off-base with spouse. Individuals in receipt of BAS must pay prescribed rates for all meals eaten in a government messing facility. The facts to be established in these cases are:

a. That the permission to ration separately was granted by competent authority.

b. The truth of the statements to which the service member certified his request to ration separately.

c. If the allegation concerns nonpayment for meals consumed in a government messing facility, ascertain dates, places, and witnesses to the consumption and the fact that payment was not made.

24-9.7. Separation Payments. Any payments, except for dependent travel, occurring under any law to any member of the uniformed service incident to his release from active duty or active duty for training, or for return home incident to release from active duty, may be paid to the service member before departure from his last duty station, whether or not he actually performs the travel involved. Current Joint Travel Regulations allow a military member being separated from active duty to draw advance travel pay for travel from the last duty to his home of record or a point of lesser distance. Legal opinions from the NCIS legal staff and a member of the DOJ are that no criminal violations have occurred when the member merely fails to submit a final settlement claim. Accordingly, no NCIS investigations should be initiated when that is the sole allegation. If, however, there is reason to suspect the member did not perform the travel for which an advance was received, and a claim submitted, an investigation should result if it meets a prosecutorial threshold. Any service member discharged under honorable conditions having accrued leave not to exceed 60 days at the time of separation will be paid for such leave. Most investigations in this area involve falsification of leave records. Investigation of these offenses involves:

(b)(7)(E)

24-9.8. Failure to Stop Allotments. Directives require that allotments be discontinued upon a service member's discharge, release from active duty, retirement, resignation, or death. Investigations in this area are usually requested to ascertain the reason the allotment was not stopped and who was responsible for its continuance. The information to be developed in these cases is:

a. When and what steps were taken by the member or responsible administrative personnel to effect a discontinuance of the allotment;

b. The reason the allotment was not discontinued and the responsibility therefore;

c. Whether the continuance of the allotment resulted from any collusive action, and the extent to which participant was involved.

24-9.9. Alteration of Military Pay Records and Related Documents. Investigations in this area are usually based on allegations that accounting and finance documents have been altered to enable a service member to obtain funds to which there was no entitlement. It is not always the service member whose particular record is involved who is guilty of altering or causing the document to be altered. Alterations may be accomplished by erasure or other deletion or addition of erroneous information on the document. The facts to be established in these cases are the type of alteration, by whom it was made, what individuals profited and whether there was any collusion in accomplishing the act. Investigative steps follow closely those in Separation Payment Investigations.

24-9.10. Misappropriation of Federal Funds by Accounting and Finance Personnel. Most investigations in this area are conducted as a result of allegations that accounting and finance personnel unlawfully have converted Federal funds to their own use. The misappropriation may be accomplished in numerous ways, but always involved is documentation which may be fictitious, altered, or destroyed. Again the investigative steps closely follow those set forth in Separation Payment Investigations.

24-9.11. Improper Payment of Training Pay to Reserve Personnel. This irregularity involves Reserve personnel not on extended active duty receiving pay for periods of training that they either did not attend or did not attend for the required number of hours to be eligible for such payment. This situation usually arises where a member of a Reserve unit signs the name of an absent member to an attendance roll, thereby enabling the latter to collect payment. The investigation should develop information to establish whether the person in question did in fact receive training and, if not, the circumstances surrounding the falsity of the attendance roll and responsibility therefore.

24-9.12. Bigamy Investigations. A bigamy occurs when a marriage is contracted at a time when one of the contracting parties has a lawful spouse, then living. Other offenses of a fraudulent nature often accompany bigamy committed by a service member, often include obtaining BAH, medical benefits, travel and other benefits for the spouse.

24-10. PERSONNEL ACTION (SUBCATEGORY 4F).

24-10.1. The following glossary of terminology applicable to this subcategory follows:

a. Enlistment, Appointment. The terms "enlistment" and "appointment" include any means of entry, except induction, into the military.

b. Separation. The term "separation," unless otherwise specified, includes discharge or any other means of discontinuing military duty.

c. Misrepresentation or Concealment. Misrepresentation or concealment may involve matters that, if truthfully stated or revealed, would induce an inquiry by the recruiting, appointing or separating officer concerning the qualifications or disqualifications for enlistment, appointment or

separation. Such misrepresented facts usually pertain to previous service, arrest records, dependents, etc.

d. Pay or allowances. Acceptance of food, clothing, shelter, pay or transportation from the government constitutes receipt of pay or allowances. On the other hand, whatever is furnished an accused while in custody, confinement, arrest or restraint pending trial for fraudulent enlistment or appointment is not considered an allowance.

e. Fraudulent Enlistment, Appointment, or Separation. An enlistment procured by means of either knowingly making a false representation in regard to any of the qualifications prescribed by law, regulation, or order, or a deliberate concealment in regard to such disqualification. The false representation or concealment is made by the person being enlisted, appointed, or separated. The false information provided must be of the nature that would preclude the person's enlistment if the person provided correct or accurate information.

f. Unlawful Enlistment, Appointment, or Separation. Knowingly and unlawfully enlisting, appointing, or separating an individual. This violation rests with the enlisting, appointing, or separating official.

24-10.2. Fraudulent enlistments, appointments, and separations are punishable under Article 83, UCMJ. The elements of proof are:

a. That the accused enlisted in, was appointed to, or separated from the armed forces;

b. That the accused knowingly misrepresented, or deliberately concealed, a certain material fact(s) regarding his qualifications for enlistment, appointment, or separation;

c. That the enlistment, appointment, or separation was procured by such false representation or deliberated concealment; and

d. That under the fraudulent enlistment or appointment, the accused received either pay or allowances, or both, as alleged.

24-10.3. Unlawful enlistments, appointments, or separations are punishable under Article 84, UCMJ. The elements of proof are:

a. That the accused affected the enlistment, appointment, or separation of the person named as alleged;

b. That the person was ineligible for such enlistment, appointment, or separation because it was prohibited by law, regulation, or order; and

c. That the accused knew he was charged with knowledge of such facts at the time of the enlistment, appointment, or separation.

24-10.4. Investigative Techniques and Procedures are set forth below:

a. Personnel Records Checks. A check of personnel records of every subject or logical suspect should be conducted and reported. It is desirable that this check be conducted prior to the interview of the subject or logical suspect, in order to further acquaint the agent with the individual's background.

b. Establishing Receipt of Pay and Allowances. The fact that a subject received pay and/or allowances should be established by documentary evidence at the finance office. If such records are not available, witnesses must be found who can testify that the subject was seen receiving food, clothing, shelter, or transportation. On occasion, the length of the appointment or enlistment may be sufficient circumstantial evidence to support the element of receipt of pay and allowance.

c. Review of Records. Almost all cases of fraudulent enlistment or separation may be established by available official records. Depending on the circumstances or facts alleged, the agent should assure that he obtains properly authenticated copies of records (arrest, prior service, identification, etc.) for use in possible judicial proceedings.

d. Recruiting and Separating Personnel. Often the personnel responsible for enlisting or separating the suspect can provide important information. In the case of an enlistment, recruiting officials often recall the individual or have retained a copy of an interview report. Similarly, separation personnel may recall information or have records which may be of value to the investigation.

e. Advancement in Rating Examination. NCIS will not initiate investigations into the suspected compromise of service-wide advancement in rating examinations solely on the basis of examination score analysis or an individual's GCT or past examination grades. Such investigations will be initiated by NCISHQ only on a very selective basis. In the event local commands request investigative assistance solely on the above rationale, they should be referred to Naval Personnel Command (NPC) who will coordinate with NCISHQ. This policy is not intended to preclude field components from initiating investigations which are based upon specific allegations of collusion/cheating not related to past examination score analyses, nor to relax any effort aimed at locating and identifying purveyors of examination questions or answers.

f. If an individual is accused of falsifying or omitting from his DD Form 398, "Armed Forces Security Questionnaire," any information having a counterintelligence significance submitted at the time of his appointment or enlistment, then the investigation will be conducted under the appropriate counterintelligence case category rather than under Subcategory 4F.

24-11. GENERAL PROCUREMENT (SUBCATEGORY 4G).

24-11.1. This subcategory is used for investigations pertaining to criminal irregularities in connection with the procurement, administration, or disposition of U. S. Government property or services that are not otherwise specifically defined as a separate case subcategory. Procurement activities involve numerous complicated and highly technical procedures. Before conducting any procurement fraud investigation, the investigator must be familiar with the procurement process and statutes and regulations applicable thereto. An orientation conducted by the local procurement

officer regarding procurement procedures, generally and highlighting particular features of local policy is a valuable aid to the investigator who is unfamiliar with the conduct of this type of investigation.

24-11.2. Small Business Administration (SBA).

a. It is the general policy of the government to aid and assist small businesses in the obtaining and execution of procurement contracts. Similarly, it is also governmental policy, whenever possible, to award government procurement contracts to contractors who will cause them to be performed in geographical areas designated by the Department of Labor (DOL) as "labor surplus areas." These two policies are interrelated and coordinated in their implementation.

b. The Small Business Act was enacted in 1953, thus creating the Small Business Administration (SBA). This independent executive agency is given the authority to foster and implement the small business policy set forth in the statute. The SBA makes general determinations of what constitutes a small business in a particular industry. In addition, the SBA will determine and certify whether a particular concern satisfies the small business criteria in order to be eligible for small business preference. The SBA will also determine whether a small business concern possesses the financial and other capabilities to render satisfactory performance on a particular procurement contract. In such cases, the SBA may issue a Certificate of Competency that certifies the "capacity" and "credit" of the concern to perform.

c. In order to carry out the congressional policy of preferential treatment for small business concerns in government procurement, a method of "setting aside" certain procurement actions has been established. Under this procedure, after a determination has been made that items to be procured are appropriate for procurement from small business concerns, a determination may be made to set all or part of the procurement aside for participation by small business concerns only. .

d. Labor surplus area concerns are so classified by their geographical location and by the concern's willingness to institute and follow approved employment programs involving hiring of disadvantaged persons. The degree of preference afforded to a labor surplus area concern depends upon its classification. These classifications are:

(1) Certified eligible with a first preference.

(2) Certified eligible with a second preference.

(3) A persistent or substantial labor surplus area concern.

(4) Not a labor surplus area concern.

e. Like the small business program, the labor surplus program can be implemented by use of the set-aside technique. Only partial set-asides (those where only a portion of the quantity to be procured is set aside solely for labor surplus participation) can be used. In this way, the benefits of a labor surplus preference may be obtained without expenditure of a premium in contract price.

f. As an adjunct to the policies discussed above, both the small business and the labor surplus program include provisions whereby contractors are encouraged or even required to subcontract with small business or labor surplus area concerns. This is accomplished by inclusion of certain clauses in contracts involving certain dollar amounts. For example, construction contractors on contracts in excess of $500,000 may be required to participate in a small business-subcontracting program.

24-11.3. Procurement Policy and Procedures.

a. The Federal Acquisition Regulation (FAR) is the primary regulation for use by all Federal Executive agencies in their acquisition of supplies and services with appropriated funds. It became effective on April 1, 1984, and is issued within applicable laws under the joint authorities of the Administrator of General Services, the Secretary of Defense, and the Administrator for the National Aeronautics and Space Administration under the broad policy guidelines of the Administrator, Office of Federal Procurement Policy, Office of Management and Budget. The FAR precludes agency acquisition regulations that unnecessarily repeat, paraphrase or otherwise restate the FAR; limits agency acquisition regulation to those necessary to implement FAR policies; and procedures within an agency and provides for coordination, simplicity, and uniformity in the Federal acquisition process. Among other matters, the FAR sets forth policies of the DOD regarding:

(1) Formal Advertising;

(2) Negotiations;

(3) Coordinated Procurement;

(4) Interdepartmental Procurement;

(5) Foreign Purchases;

(6) Contract Clauses;

(7) Patents and Copyrights;

(8) Bonds and Insurance;

(9) Federal, State, and Local Taxes;

(10) Labor;

(11) Government Property;

(12) Inspection and Acceptance; and

(13) Contract Cost Principles.

b. The DOD FAR Supplement (DFARS) is codified within the same regulation that created the FAR and makes the regulations found in the FAR applicable to the DOD. Neither the FAR nor DFAR applies to transportation services purchased by transportation requests, transportation warrants, bills of lading, and similar transportation forms. Purchase of these excepted transportation services shall be in accordance with specific regulations and instructions issued by the Surface Deployment and Distribution Command, formerly (Military Traffic Management Command), Military Sealift Command, Air Mobility Command (formerly Military Airlift Command), and the Departments. Revisions to the DFAR are issued through the Defense Acquisition Circulars (DAC). The DFARS contains regulations that focus only on requirements of law, DOD-wide policies, delegations of FAR authorities, deviations from FAR requirements and policies, and procedures that have significant effect beyond internal DOD operating procedures. DOD internal procedures and other information that does not require implementation by formal regulation is found in the DFARS-Procedures, Guidance, and Information (PGI). Further information and updates to the FAR, DFARS, and PGI can be found on the Defense Procurement and Acquisition Policy Website at www.acq.osd.mil/dpap/index.htm.

c. The DON's supplement is known as the Navy Marine Corps Acquisition Regulation Supplement (NMCARS) and establishes for the DON Uniform Policies and Procedures for the acquisition of supplies and services. The NMCARS is not intended to be a "stand alone" document and therefore, it must be read with the FAR and DFARS. The NMCARS is updated and revised through the Navy Acquisition Circulars (NAC).

d. The Naval Supply Systems Command (NAVSUP) (www.navsup.navy.mil) also provides implementation guidance to the smallest purchasing office in the field. It provides local commands more specific information concerning the requirements of FAR, DFARS and NMCARS as they relate to procurement in the DON.

e. Responsibility for procurement.

(1) The Assistant Secretary of the Navy Research, Development, and Acquisition have the Navy staff responsibility for procurement and production including procurement policy. Copies of relevant policy documents can be found on DON Acquisition website www.acquisition.navy.mil.

(2) Heads of procurement activities are responsible for the procurement of all supplies and services. They are responsible for the direction and control of the purchasing offices of their activities and for effective coordination with related activities.

(3) Contracting officers at contracting and purchasing offices are authorized to enter into contracts for supplies or services on behalf of the government by formal advertising, by negotiation, or by coordinated or interdepartmental procurement.

f. Organization.

(1) Before the agent can undertake an investigation of procurement irregularities, he must acquire a working knowledge of pertinent procurement procedures and the organizational

structure of a purchasing office. Such knowledge will give the agent a sound factual basis of information from which to launch an investigation. Maximum use must be made of the FAR and related documents.

(2) The Congress of the United States must enact enabling legislation that provides a procurement agency with the necessary legal authority to act. Such enabling legislation is comparatively brief, setting forth the broad intent of the government. The procurement agencies of the Executive Branch promulgate their own implementing directives and regulations based on the legislation. These implementing publications serve as detailed guides to procurement activities, and must conform to the intent of the basic legislation.

24-11.4. Irregularities in The Procurement Process Requiring Investigative Actions.

a. Contractor. Contracts embrace all types of agreements for the procurement of supplies and services. Part 52 of the FAR sets forth clauses required in all military procurement contracts as well as optional clauses to be used when applicable, e.g., as in fixed-price supply contracts, cost-reimbursement type supply contracts, and fixed-price research and development contracts. Special clauses used for personal services contracts are also included. Each of these clauses, if contained in a contract, binds the contractor in some way. Mere failure to comply with a contractual provision is not indicative that fraud has necessarily been committed.

b. Bidders. Certain noncompetitive practices may originate among bidders, e.g., collusive bidding, follow-the-leader pricing, rotated low bids, uniform estimating system, sharing of the business, identical bids, etc. (see case subcategory 4A).

c. Government Personnel-Malfeasance, Misfeasance, and Nonfeasance.

(1) Malfeasance. Government personnel engaged in the procurement process may violate provisions of the criminal code or specific statutory prohibitions and concomitant administrative regulations through actions such as accepting gratuities or conspiring to defraud the government. This conduct would represent a wrongful act and malfeasance in the performance of duty and may be both legally and administratively actionable upon the establishment of requisite facts (see subcategories 4C and 4H).

(2) Misfeasance. Government procurement personnel in the course of performance of their duties may perform a lawful act but in a manner prohibited by governing regulations or perform the act in a manner not in accordance with that specifically directed in such regulations. Actions of this nature constitute an act of misfeasance and would be administratively actionable. In the case of military personnel, these actions would be actionable within the provisions of the UCMJ.

(3) Nonfeasance. In the event government procurement personnel fail to do something procedurally required by procurement regulations during the course of the performance of their duties, they are guilty of nonfeasance. Even if such omission were not part of any scheme to defraud or otherwise injure the government, it nevertheless would be actionable as in the case of misfeasance.

(4) Significance. Many provisions of the FAR have been carefully designed as safeguards to prevent acts of malfeasance or other injuries to the government. Malfeasance or nonfeasance opens the door to and may encourage or incite frauds or other acts injurious to the public interest.

24-11.5. Investigative Interest and Consideration.

24-11.5.1. General.

a. One of the major difficulties in any procurement investigation is that irregularities, if any, often occur within the framework of a complex pattern of statutory provisions, administrative regulations, and departmental or agency procedures. Only with a reasonable familiarity with these laws, regulations, and procedures can the agent recognize failures to follow directives, misapplication of regulations, or other deviations from normal procurement processes. This familiarity with the governing laws and regulations is a basic tool to be employed in exploring the causes and contributing factors in procurement irregularities. It is imperative that the investigation be "scoped" or its parameters defined so that the investigation of specific, citable criminal statutes can be undertaken from the onset of the investigation.

b. Administrative and criminal violations often go hand in hand. A breakdown in administrative procedure provides a suitable climate and convenient cover for unlawful manipulations of the procurement process. Deviations from established procedure may be indicative of criminal irregularities, serious administrative errors, or both. On the other hand, limited deviations may at times have little significance and may actually facilitate a particular procurement action.

c. Procurement irregularities do not occur at set points in time. Discovering such irregularities requires continuous scrutiny of actions taken, from the inception of the procurement action to the termination of the contract(s). A clear-cut case with easy identification of the exact spot where an irregularity occurred is a rarity. More often, a critical scrutiny of each step in the procurement process must be undertaken. Decisions made by supply, engineering, or maintenance personnel may have a direct bearing on a contract award.

d. Although administrative deficiencies may lead to loss of funds or culpable negligence, once it has been established through investigation that no criminality exists, the NCIS investigation should be terminated. If it is apparent that faulty administrative procedures exist, the command should be apprised in order that command action may be initiated to uncover and correct these deficiencies.

24-11.5.2. Vulnerable Actions and Areas. The following are some operational actions and areas worthy of close scrutiny by the agent in pursuing inquiries into allegations of irregularity in the procurement process:

a. Actions by government employees.

(1) The pre-award survey inspections may have been inadequate or the reports of

inspection of the contractor's facilities may be false or misleading.

(2) Premature or unauthorized release of procurement information.

(3) Permitting contractors access to areas or offices where procurement actions are planned or discussed and where pre-release information may be obtained.

(4) Failure of contracting officers or other administrators to furnish boards of awards with all pertinent information.

(5) Questionable use of contracts which permits price redetermination after the contract has been negotiated.

(6) Failure of boards of awards to consider all relevant factors, particularly when the senior, best-informed, or dominating member is in a position to exert undue influence.

(7) Failure of contracting officers or other administrators to fully enforce the provisions of a contract, particularly as it pertains to inspections, delivery of government-furnished property, delivery schedules, or closing of completed contracts.

(8) Inspectors failing to make required inspections of contractor products; permitting the contractor to use inferior materials; allowing contractors to meet weight specification by the addition of unauthorized materials; or allowing contractors to weaken an item or material by failure to meet weight or density specifications (see case subcategory 4P).

(9) Release of government-furnished property to a contractor before it is needed, thus enabling the contractor to use it on other products; failure to supervise properly the use of government-furnished or government-owned property; or failure to exercise adequate controls over or accountability for such property, particularly upon completion of a contract.

(10) Failure of the contract administrator to document the contract file, particularly concerning actions which could result in savings to or be detrimental to the interest of the government.

b. Actions by contractors.

(1) Giving gratuities to government employees, with or without intent to bribe. Such gratuities may be very minor items at first, gradually increasing in value until the employee is under definite obligation to the contractor (see case subcategories 4C and 4H).

(2) Frequent visits or telephone calls, official and/or social, to government employees during and after duty hours, thereby possibly acquiring information which will result in a more favorable position for the contractor.

(3) Substitution of rejected or substandard items for acceptable items in shipments with or without the inspector's knowledge (see case subcategory 4P).

(4) Presenting false financial or production capability data or other incorrect information prior to the award of a contract. Such false information may sometimes be given a cloak of apparent truth by employing such tactics as borrowing funds or materials or exhibiting facilities and equipment belonging to some other firm. (See case subcategory 4D.)

c. Operational areas.

(1) Specifications. Proprietary specifications or specifications so slanted as to favor the product of a particular manufacturer may be used.

(2) Sole source procurement. Sole source procurement must be thoroughly justified; they may be questionable because of the possibility of individuals in such areas as engineering, supply, maintenance, etc., inserting their own self-interests.

(3) Common types of irregularities.

d. Favoritism. An allegation or a report of favoritism may be on a specific, isolated incident, and, thus, may present relatively simple investigative problems. On the other hand, such an allegation may be vague and general and require extensive study, evaluation, and records checking to pinpoint an issue definitely sufficient for specific investigation.

e. Gratuities (see case subcategories 4C and 4H). The prohibition upon the giving or receiving of gratuities in connection with procurement actions applies to all persons involved in the process. The investigative approach to allegations involving gratuities includes:

(1) Establishment of the giving or receiving of the gratuity.

(2) Determination of the status of the alleged receiver, e.g., contract administrator, inspector, originator of the procurement request, pricing analyst, etc.

(3) Ascertaining and securing the statements of witnesses and other persons aware of the facts and related data.

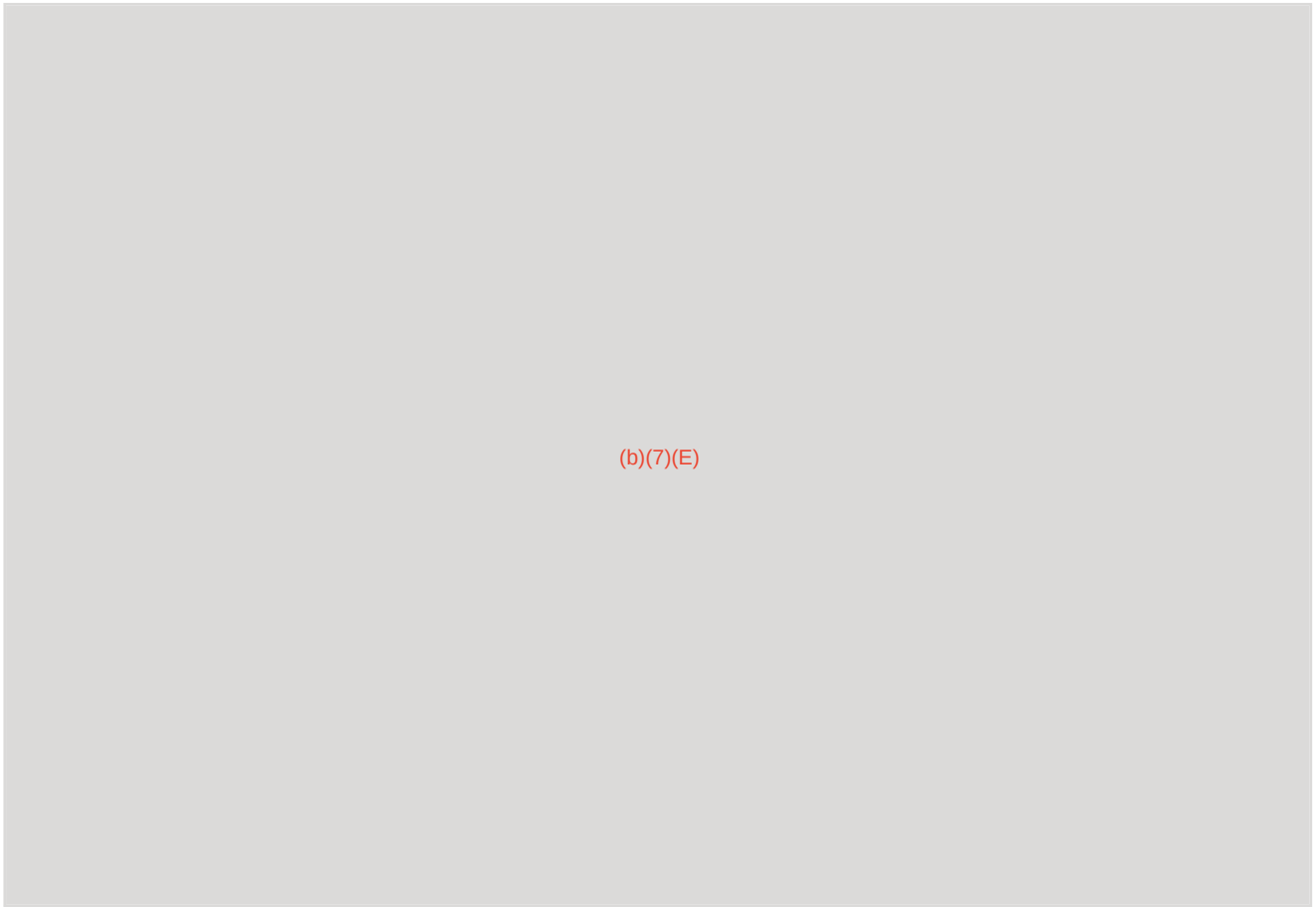
(4) Securing statements of the alleged receiver and donor.

(5) Securing documentary proof and corroborative data when possible.

24-11.5.3. Premature Release of Information. All prospective contractors should be treated equally. Such treatment is essential to effective competition and the securing by the government of the most favorable pricing and other factors contributing to the determination of the bid or proposal most advantageous to the public interest. Cost analysis by a prospective contractor in regard to any given procurement may take considerable time and involve appreciable expense. It is to the best interests of the government that all prospective contractors be given ample and equal time, under the terms of the Invitation for Bid (IFB) or the Request for Proposals (RFP), to permit efficient cost and price analysis and forecast of production capability. The "leaking" of information, whether inadvertent or

intentional, to a prospective contractor prior to the regular release of information regarding a proposed procurement can give undue advantage to the one so favored. If this "leaking" is combined with a relatively short time between the regular release of IFB or RFP and the date for submission of bids or proposals, particularly in the case of complex procurement items, only the pre-informed contractor may be in a position to bid effectively. The result may be that the contract is "steered" to this favored contractor, possibly at a serious disadvantage to the government. All information regarding prospective procurement, funds allotted, and government estimates of costs should be closely guarded. Procurement information may be released, within established procedures, only by contracting officers and their authorized representatives, contract assistants, ordering officers, and imprest fund cashiers. The investigation of allegations of irregular release of information is difficult because of the numerous possible sources of such information, including persons with only minor operational responsibilities, e.g., stock clerks, typing personnel, persons providing administrative or technical assistance.

24-11.5.4. Conflict of Interest. There should be no conflict between the private interests of procurement personnel and the public interests of the government. Both administrative regulations and criminal laws prohibit such conflict. In the case of allegations of conflict of interest, the agent should isolate the type of violation and identify the law or regulation involved. If it is apparent that a possible violation has occurred, the agent should review relevant personnel records, personal history statements, and similar documents, and interview the persons apparently involved in order to establish clearly whether such a conflict of interest actually occurred and to determine its exact nature, i.e., intentional or inadvertent, criminal, or administrative (see case subcategory 4C).



(b)(7)(E)

24-11.5.6. Fraud in the Disposal of Government Property.

a. Closely aligned with the investigation of frauds against the government perpetrated during the procurement process are fraudulent acts that take place when disposal of that property occurs. The proper procedure for the disposal of supplies and equipment is outlined in DOD 4160.21-M, the Defense Materiel Disposition Manual, dated 18Aug97. This regulation should be examined before undertaking an investigation of suspected impropriety in the disposal process. The techniques recommended for investigating procurement fraud will normally apply to the disposal situation as well.

b. Personnel Frequently Involved in the Fraudulent Disposal of Government Property. Government personnel who may be involved in the fraudulent disposal of government property include those who are responsible for:

(1) Acquiring government property, managing receipts for internal transfers, and distributing it for use by individuals, units, or organizations; reporting government property as not fit or needed for use by the unit or agency to which it is issued;

(2) Inspecting the property and classifying it as unfit or unneeded;

(3) Announcing to potential buyers that the property is for sale and requesting bids or proposals to buy; and

(4) Consummating sales and supervising and reviewing disposal actions.

24-11.5.7. Vulnerable Actions and Areas. The following are some areas worthy of close scrutiny by the agent in pursuing an investigation into allegations of irregularity in the disposal process:

a. Unauthorized Non-sale Disposition or Diversion by Government Employees.

(1) Irregular business practices.

(a) Lack of supervision at shipping and receiving points and failure to properly record the transactions.

(b) Use of personal contract methods without the keeping of records.

(c) Unusual concentration and exercise of power in the hands of one person or one group to the detriment of established functions and powers of duly authorized officials. Closely akin to this situation is the performing of one official's functions by another, either on a regular basis or on a personal favor basis. Because different functions are performed by different persons, there

are effective checks and balances. Any situation in which this principle is ignored to the extent that one person is put in the position of performing all essential tasks connected with a transaction, and in effect, approving his own actions, should be viewed with suspicion.

(d) The temporary borrowing, without good reason, of property between DON activities.

(2) Irregular business conditions.

(a) Chronic shortages. Chronic shortages in a command, despite normal procurement and receipt of items claimed to be in short supply, may indicate that items are being wrongfully diverted from their intended purposes or that they are not being received in the quantities alleged. The agent may be alerted to this situation if some units encounter no difficulty in securing needed items while others with similar needs and justifications regularly have their requisitions returned unfilled. The necessity for having personal influence with those in a position to issue Navy supplies and equipment may be an indication that frauds are being perpetrated.

(b) Maximum use of droppage allowances. The regular use of maximum droppage allowances may indicate attempts to conceal fraud. If the supplies are actually delivered in the quantities the government pays for and are wrongfully disposed of after being received, there may be larceny and not fraud. On the other hand, if the supplies that are being written off were never received, despite the fact that the government paid for them, there may be fraud, probably by collusion between the contractor and the personnel responsible for procuring and receiving the supplies. Of particular importance with regard to this practice are the offenses outlined in Article 132, UCMJ. Article 132 makes it a crime to fraudulently deliver less than an amount called for by receipt and prohibits the making or delivering of a receipt without full knowledge of its content when done with the intent to defraud the government. Falsified records of issue; unfounded allegations of theft, spoilage, or other loss; or falsified accounting records and inventories may also indicate fraud or larceny.

(c) Unusual personnel turnovers. The padding of payrolls, the mass hiring and firing of employees, mass resignations of personnel, or unusually low personnel turnover and chronic requests for transfers by personnel may be indications that all is not well in a unit or facility. Honest personnel may quit or ask to be transferred when they realize that illegal transactions are being made. An unusual desire to get into or remain with a unit or facility, or the unusual desire of a supervisor to secure or keep particular individuals, may be an indication of fraud.

(d) Irregular inventories. The regular appearance of shortages or overages near the maximum allowed; irregularities in the taking of inventories; attempts to influence the selection of persons to take inventories; the fact that the same persons are repeatedly assigned to inventory at the same facility; attempts to confuse or deceive officials designated to make inventories; and the appearance of certain articles at inventory time coupled with an inability of using units to secure them by requisition shortly thereafter, may indicate fraud. Perfect inventories or accountings should also be viewed with suspicion.

(e) Repeated reports of larcenies, burglaries, etc. Repeated reports of these

offenses may indicate that responsible personnel are inventing these offenses for the purpose of laying the groundwork for writing off materials by means of reports of survey.

(f) Statements of charges and reports of survey. The excessive use of these procedures to justify the absence or loss of military property may indicate that military property is being diverted for personal gain. A fraudulent report of survey may be initiated anywhere and at any time since the person is actually seeking relief from pecuniary liability for property. However, a fraudulent statement of charges is not likely to be made except when the property will bring the offender more when sold than the regular price he must pay the government. This situation may exist in any area in which the economy is disturbed. Statements of charges may also be initiated by persons on articles of military property that they want, but cannot procure through normal civilian channels.

(g) Materials on the black market. The appearance of materials on the black market, coupled with the absence of reported thefts, shortages of similar military supplies, or absence of other sources from which black marketers could obtain similar items, may indicate the government property is being diverted.

(2) Unauthorized Disposal of Government Property by Sale.

(a) Failure to notify interested buyers or adequately advertise the sale.

(b) Falsification of eligibility of buyers in instances where sale is restricted by law to certain categories of persons or agencies, where the bidder is ineligible by reason of collusion with other bidders, or where the bidder is debarred from contracting under DOD regulations.

(c) Sale of property at unreasonably low prices.

(d) Sale of serviceable property as damaged, unusable, or non-repairable.

(e) Mixing of serviceable and unserviceable property and sale of the mixture at prices appropriate only for unserviceable property.

(f) Concealing of valuable items or parts in property sold as unfit or unserviceable.

(g) Repair of property at government expense prior to its sale at prices appropriate for unserviceable property.

(h) Permitting a buyer to hand-pick items advertised for sale "as is" in general lots.

(i) Providing information to one bidder that is not furnished all bidders (quantitatively or in point of time).

(j) Solicitation and/or submission of spurious bids in an effort to create an

impression of competition.

(k) Substandard demilitarization of property where demilitarization is required.

24-12. BRIBERY (SUBCATEGORY 4H).

24-12.1. General. Bribery is the corrupt giving to, asking for, or receipt by government personnel or anyone acting for or on behalf of the United States of anything of value:

a. To influence an official act;

b. To influence the commission of or collusion in any fraud on the United States; and

c. To induce violation of official duty.

It includes the corrupt giving to or receipt by a witness of anything of value to influence his testimony under oath or to influence his absence from a trial, hearing, or other proceeding. It further includes payments to and receipts by such personnel "for" or "because of" an official act or testimony or absence from a trial, hearing, or proceeding at which testimony was to be given.

24-12.2. Article 134, UCMJ, concerning bribery and graft are similar in nature to 18 USC 201, which addresses the matter of bribery and makes it applicable to all persons performing activities for or on behalf of the United States. Section 201 describes the elements of the statutory violations, and these should be used as a guide during the course of bribery investigations.

a. Discussion.

(1) "Public Official," as used in Section 201, means all government officers and employees, jurors, and any person acting for or on behalf of the United States, or any department, agency, or branch of government thereof, in any official function, under or by authority of such department, agency, or branch of government. This definition covers even persons who perform activities for the government through a contractual arrangement.

(2) "Official Act" means any activity that a public official undertakes for the government.

(3) "Anything of value" means any thing that can be offered or given as a bribe.

(4) In subsection 201(b), with respect to the intents with which a bribe may be offered, the phrase "to influence any official act" is broad enough to cover a bribe offered or given to one official even though the official action sought to be influenced may be that which a second official must take. The word "corruptly" means with wrongful or dishonest intent. This subsection also forbids an attempt to influence a public official by an offer or promise of something of value from which the public official himself will not benefit, but which will be of advantage to somebody else.

(5) Subsection 201(c) outlines the three alternate purposes for which a bribe may be

sought. The language in this subsection emphasizes that it is the purpose for which the recipient knows the bribe is offered or given when he solicits, receives, or agrees to receive it which is determinative of criminality. The subsection punishes the public official not only for soliciting or receiving anything of value, but also for doing such acts for any other person or entity. This subsection covers only the public official's own performance of any official act.

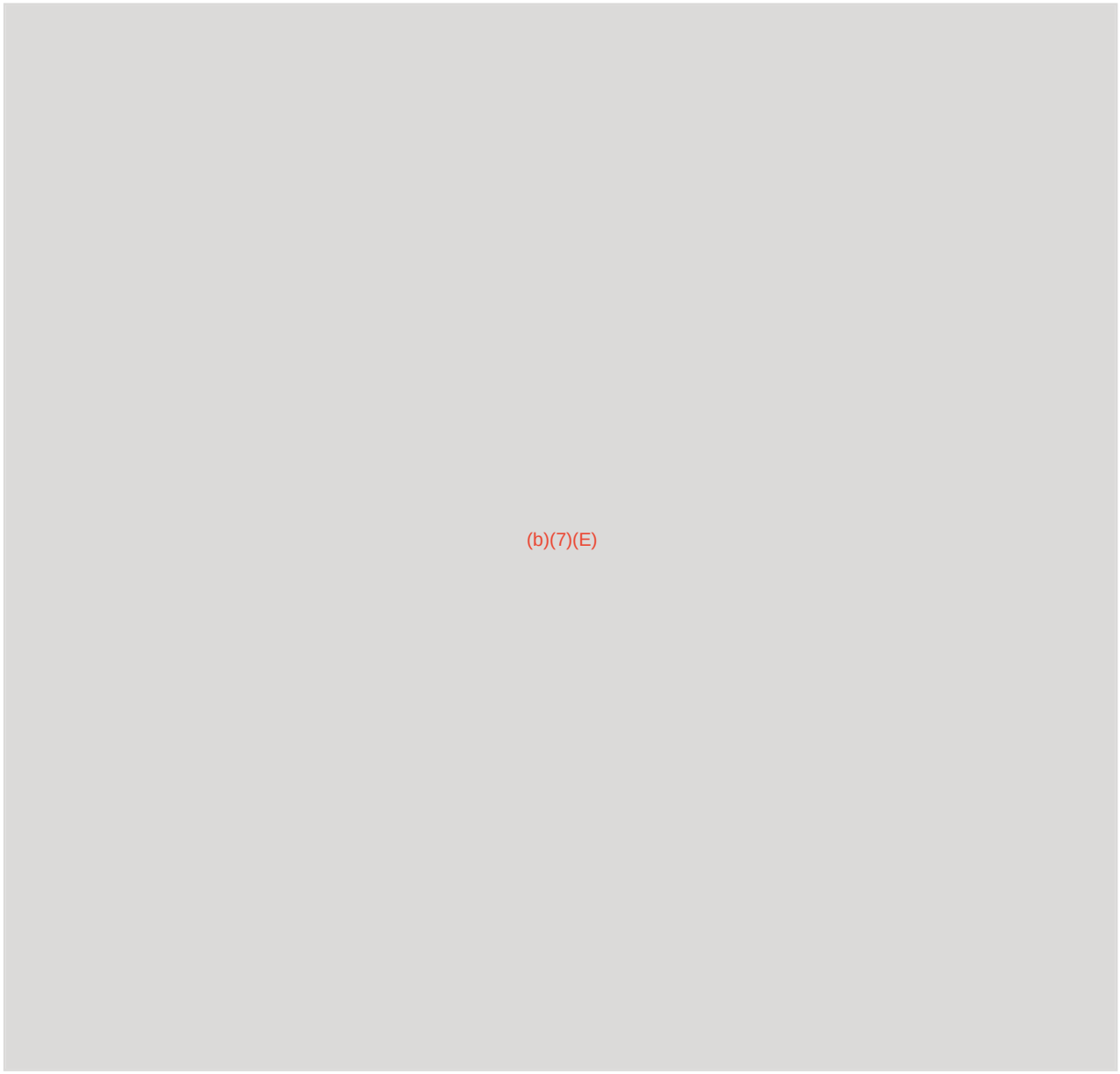
(6) Subsection 201 (d) and (e) apply the prohibitions of subsection 201 (b) and (c) to witnesses in any proceeding or before any officers authorized to take testimony, to the extent that the bribe is paid or accepted with intent to influence the witness' sworn testimony or to influence him not to testify. These subsections forbid attempts to influence a witness by an offer or promise of something of value which will be of advantage to someone else and for which the witness may not benefit.

(7) The penalties for violating subsection 201 (b) through (e) are a maximum fine of $20,000 or three times the value of the bribe, whichever is greater, or a maximum imprisonment of 15 years, or both. Additionally, the court is given the discretion to disqualify the person convicted from holding public office.

(8) Section 201, both as to persons covered and acts prohibited, has the effect of making bribery out of some situations which formerly were only gratuity matters, at most, under laws and regulations applicable to the DON. For example, if a contracting officer properly awarded a contract to a contractor, and the latter offered or gave a television set later to the contracting officer in appreciation for the contract legitimately received, this would not constitute bribery under the old statute because of the lack of intent to influence. This would have been treated as a gratuity. Under the new statute, however, this same situation would constitute bribery because the thing of value was offered or given to the contracting officer for or because of "an official act performed by him." Technically, anything of value furnished directly to DON military and civilian personnel for or because of official acts they have performed or are to perform, may constitute bribery. As a practical matter, however, it is doubtful if the furnishing of meals, drinks, and advertising items, e.g., cigarette lighters, will ever be treated other than as furnishing of gratuities. On the other hand, lavish entertainment, vacations at contractor's expense, transportation expense, and the like, furnished directly to DON personnel for or because of their official acts performed or to be performed may result in a prosecution for bribery. No hard and fast rules can be laid down as to which gifts furnished to DON personnel for or because of their official acts, will constitute bribery, and which will be considered gratuities. Each case will have to be decided on an individual basis.

24-12.3. Investigating Bribery.

(b)(7)(E)



24-13. DEPENDENCY ASSISTANCE (SUBCATEGORY 4I).

24-13.1. General. 37 USC 401 and 403 provide for service members with eligible dependents to receive a basic allowance for housing (BAH). Eligible dependents are classified in this law as: (1) primary dependents, and (2) secondary dependents. Information within this section will further define and classify dependents as well as to provide guidance with respect to required coverage in dependency assistance investigations.

24-13.2. Background. An allotment and a BAH should not be confused. An allotment is voluntary on the part of a service member and represents a part of his pay and allowances designated by the service member as payable to a financial institution, relative, church, etc. A member may also provide support to a dependent by means other than an allotment. An eligible dependent may receive support in the form of BAH. Administrative support personnel can determine whether a

member has a BAH allotment in effect to the dependent, but they are often not able to determine whether the claimed dependent, i.e., parent, is using the BAH allotment for his support, or whether they are returning all or part of the BAH allotment to the service member for his personal use. Further, administrative support personnel are not always able to verify the amounts, dates, and method of support furnished to an eligible dependent by means other than an allotment, i.e., Supplemental Security Income (SSI) pension, disability, or employment. Therefore, the NCIS must verify through investigation the actual support provided by a member instead of relying on the dependency affidavit or other information furnished solely by the dependent.

24-13.3. Definitions.

a. Primary Dependent. A person whose eligibility can be determined on the basis of relationship alone, such as a spouse or legitimate child, although entitlement to allowances such as BAH may not exist due to other factors. Examples of the latter include the dependent in occupancy of government quarters; spouse in military service; whereabouts of dependent unknown; relief from support by mutual agreement and/or court order. A service member may be entitled to BAH on behalf of any of the below listed dependents, and the primary dependents themselves are entitled to the benefits as shown:

(1) Spouse. Dependent's ID card, travel at government expense, housing.

(2) Son/Daughter (over 21 years of age).

(a) If the child is a full-time student, however there is no BAH entitlement for the service member if child is the only dependent claimed. The member's BAH entitlement would cease on the day prior to the 21st birthday. The child is entitled to dependent's ID card only. There is no entitlement to travel at government expense. Entitlement to government housing is at the discretion of the local base commander.

(b) If incapacitated, the service member's BAH will continue even if the child is the only dependent claimed. The child is entitled to a dependent's ID card and travel at government expense. Entitlement to government housing is at the discretion of the local base commander.

(3) Adopted child. Dependent's ID card, travel at government expense, and housing.

(4) Step child. Dependent's ID card, travel at government expense, and housing.

b. Secondary Dependent. A person whose eligibility must be determined on the basis of relationship and a degree of dependency on the military member. Secondary dependents may include parents, adoptive parents, stepparents, persons acting in-loco-parentis, parents-in-law, stepchildren, and illegitimate children. When meeting the required criteria, secondary dependents are entitled to the benefits set forth below:

(1) Mother/Father.

(a) Member is entitled to BAH.

(b) Dependent is entitled to dependent's ID card with Medical Service (MS), Commissary (C), Exchange (EU), and Theater (T) privileges; travel at government expense; and housing.

(2) Parents-in-law.

(a) No BAH entitlement to member.

(b) Dependent is entitled to dependent's ID card with MS, C, and T privileges.

(3) Loco parentis (any person who has stood in place of a parent to the service member at any time for a continuous period of five (5) years or more during the time the service member was a minor).

(a) Member is entitled to BAH.

(b) Dependent is not entitled to ID card, travel, or housing.

(4) Illegitimate Child.

(a) Member is entitled to BAH.

(b) Dependent is entitled to ID card with Medical Civilian Care (MC), MS, C, EU, and T privileges, and travel only if child is part of member's household.

24-13.4. Criteria For Entitlement To BAH.

a. Parents. One of the requisites for determining dependency of a parent is a completed Parents Dependency Affidavit, DD Form 137-3. In order to qualify for dependency status, it is a requirement that support provided a parent defray more than one-half the total monthly expenses of the parent. For example, if the income of a parent from sources other than the member is sufficient to defray more than one-half of the parents' expenses, dependency cannot be established, i.e., monthly expenses of $550.00 and income of $300.00. However, if the income of the parent from sources other than the member is less than one-half of the expenses, eligibility may exist provided the member has been contributing an amount sufficient to cover more than one-half of the listed expenses, i.e., expense of $550.00 and income of $225.00, and the member's contribution is $325.00. It should be noted there is not a requirement that the member's contribution be the amount of the monthly BAH entitlement if a lesser amount is sufficient to cover more than one-half of the listed expenses. Payments from Social Security, Supplemental Security Income (SSI) Veterans Administration, pensions, insurance, and other forms of annuities (stocks, dividends, and savings accounts) are considered as income for adjudication purposes. The income and expenses of both parents, unless legally separated, must be considered together as a unit even though the member may not have listed both parents on the application. Assistance from local, state, or federal agencies such as Aid to the Blind, Welfare, Aid to Dependent Children (ADC), Aid to the Disabled, or Red Cross are considered as charity and not income.

b. Illegitimate Children. To qualify for BAH in behalf of an illegitimate child, the member must provide support to the actual physical custodian of the child in the same amount of the monthly BAH if the member is assigned to government quarters. If the member is not in government quarters, he is therefore entitled to BAH at the "without dependent rate" (a lesser amount than the "with dependent rate") which is adjusted according to rate/grade. The practice of Navy Family Allowance Activity (NFAA) is to request support of at least the difference between the two rates; and as stated above, the support must be furnished to the actual physical custodian of the child. In all cases, the member must submit proof of parentage such as the child's birth certificate and a sworn statement of paternity. If the child is in the member's custody, the proof of parentage is still required but the support requirement is fulfilled through residency. All support provided by the member to the custodian of an illegitimate child must be used for the monthly expenses of the child. In other words, the money must be used for current support and not for future support, i.e., educational fund, savings account, etc.

c. Impact of Outside Income. Supplemental Security Income (SSI), Social Security employment salaries, and retirement pensions are all considered as income when adjudicating parent dependency cases. Welfare, to include unemployment compensation, is considered a charity. When information is developed revealing the dependent is receiving any type of welfare, less SSI, the pertinent agency is notified by NFAA of the amount of support being contributed by the DON. Child support received by a parent in behalf of minor children in the household is applied against the child's/children's share of the household expenses. With cases involving illegitimate children, it is required that the member furnish as proof of support at least the amount of the BAH or the difference in rates if he is not entitled to the full BAH rate. Whenever information is surfaced that any welfare agency is providing payments in the child's behalf, NFAA will notify the agency of the amount of support being provided by the DON. An illegitimate child is entitled to dependent's ID card with civilian medical privileges (MC) and uniformed services and facilities (MS).

24-13.5. Investigative Considerations. Offenses associated with dependency assistance investigations may include UCMJ Articles 81 (conspiracy), 92 (failure to obey order or regulation), 107 (false official statements), 121 larceny and wrongful appropriation), 132 (frauds against the United States), and 134 (General Article). For non-military culpable parties, 18 USC 371 (conspiracy to commit offense or defraud United States) and 18 USC 1001 (false official statements) may pertain.

a. Dependency Assistance investigations do not require complete itemization of household furnishings and personal belongings. However, a very brief statement in the body of the investigative report describing the residence, its location, condition, and contents is appropriate. When attempting to verify expenses, the agent should request and sight all receipts supportive of what is claimed. Merely confirming or obtaining an affirmative reply from the dependent concerning the information submitted on the DD Form 137-3 is not sufficient since this latter information may be untruthful or inaccurate. Since the receipt of welfare payment is considered a charity and not income by the DON, the agent should not routinely make inquiries at the various state and federal welfare agencies. The agent should, however, make pertinent inquiries of the sources contacted during the course of the investigation concerning any welfare being received by the child and/or custodian. Both negative and positive responses should be reflected in the

investigative report. Whenever there is an indication of welfare assistance, the names and addresses of the respective agencies should be reflected in the ROI whenever possible.

b. When conducting dependency assistance investigations, the following investigative techniques should be applied:

(1) Parents.

(a) Interview each.

(b) Verify all expenses by itemizing each. The verification must be independent of the information contained in the Parent's Dependency Affidavit (DD Form 1733) previously completed by the parent.

(c) Determine amount and sources of all income. This may necessitate the obtaining of financial and welfare release waivers.

(d) Determine type of health care program/insurance the parent has.

(e) Determine if the parent is employed in any capacity. Also determine if the parent is utilized as a housekeeper, babysitter, etc., for the service member.

(2) Illegitimate children.

(a) Physically sight the child.

(b) Attempt to obtain outside verification that the child resides where the service member claims.

(c) Determine the residence has clothing, toys, etc., which tend to support that a child is residing there.

(d) Verify and itemize the amount of all monthly expenses for the child. This will include any savings account or educational fund established for the child.

(e) Determine any source of outside income on behalf of the child. This may necessitate obtaining pertinent release waivers.

(f) Determine amount, method, and length of time the custodian of the child has received support payments.

(g) Determine from whom the custodian receives the support payment.

24-14. FORGERY (PERSONAL) (SUBCATEGORY 4J) AND FORGERY (GOVERNMENT) (SUBCATEGORY 4K).

24-14.1. General. Forgery is the false making or altering of a written document with intent to defraud. The discussion of the various forgery situations and investigative procedures are essentially identical for the two case subcategories, "FORGERY (PERSONAL)" (subcategory 4J) and "FORGERY (GOVERNMENT)" (subcategory 4K), the difference being whether or not the U. S. Government suffers loss or is otherwise victimized. To further clarify the difference between these two case subcategories, in cases where individuals forge U. S. Government checks and attempt to cash them, but are not successful, the investigation should be reported under the 4J subcategory since there is no loss to the government. Also, losses for checks cashed at some overseas banking institutions which have contracts with the U. S. Government to provide banking services to U. S. Forces are absorbed by the U. S. Government; in cases where such an agreement is in effect, the 4K subcategory should be used.

24-14.2. Forgery may be committed either by falsely making a writing or knowingly uttering a falsely made writing. There are certain aspects common to both aspects of forgery, which are:

a. A writing falsely made or altered;

b. An apparent capability of the writing so falsely made or altered to impose a legal liability on another, or change his legal right or liability to his prejudice; and

c. An intent to defraud.

24-14.3. Forgery is not committed by the genuine making of a false instrument for the purpose of defrauding another, although such a situation may be investigated under these case subcategories. An example is the writing of a check on a closed account by the former account holder. A check bearing the signature of the maker, although drawn on a bank in which the maker has no money or credit, and even with intent to defraud the payee or the bank, is not forgery because the check, though false, is not falsely made. Signing the name of another to a check without authority and with intent to defraud, however, is forgery, as the signature is falsely made.

24-14.4. A forgery may be committed by a person signing his own name to an instrument. For example, if a check payable to the order of a certain person comes into the hands of another person of the same name, the receiver commits forgery, if, knowing the check to be another's, he endorses it with his own name, intending to defraud. Forgery may also be committed by signing a fictitious name, as when a person makes a check payable to himself and signs it with a fictitious name as drawer.

24-14.5. Some of the instruments that are most frequently the subject of forgery are checks, orders for delivery of money or goods, military orders directing travel, and receipts. A writing may be falsely "made" by materially altering an existing writing, by filling in a page signed in blank, or by signing an instrument already written.

24-14.6. The writing must appear on its face to impose legal liability on another; for example, a check or note, or to change a legal right or liability to the prejudice of another, as a receipt. The false making with intent to defraud of an instrument affirmatively invalid on its face is not forgery because it has no legal efficacy. However, the false making of another's signature on an instrument,

with intent to defraud, is forgery even if there is no resemblance to the genuine signature and the name is misspelled. It is not forgery to make falsely or alter with intent to defraud a writing which does not operate to impose a legal liability on another or change a legal right or liability to his prejudice, as for example, would ordinarily be the case where a mere letter of introduction is involved.

24-14.7. Proof In Forgery Cases. Under Article 123 (forgery), UCMJ, it must be proved:

a. That a certain signature or writing was falsely made or altered, as alleged;

b. That the signature or writing was of a nature that would, if genuine, apparently impose a legal liability on another or change his legal right or liability to his prejudice;

c. That it was the accused who falsely made or altered such signature or writing; or uttered, offered, issued, or transferred it, knowing it to have been so made or altered; and

d. That the accused intended to defraud.

e. In proving forgery, the instrument itself should be produced, if available. That the signature to a written instrument was falsely made may be provided by the testimony of the person, whose signature was forged, showing that he had not signed the document, and that he had not authorized the accused to do so. If the name of a fictitious person is used as, for example, the purported drawer of a check, show that the fictitious person has no account in the bank upon which the check was drawn.

f. Various federal violations may also be included under case subcategories 4J and 4K. They may include 18 USC 471 (obligations or securities of United States), 500 (Money Orders), 510 (forging endorsements on Treasury checks or bonds or securities of the United States), 641 (Public money, property, or records), 661 (special maritime and territorial jurisdiction), 1025 (false pretense on high seas and other waters), 1028 (fraud and related activity in connection with identification documents, authentication features, and information), 1029 (fraud and related activity in connection with access devices), 1341 (frauds and swindles), and others. The specific applicable statutes(s) should be cited upon the initiation of all forgery related investigations.

24-14.8. Investigative Procedures In Forgery Cases.

a. The usual forgery investigation by the NCIS involves checks, orders, discharge papers, birth certificates, notices of promotion, and similar documents. The investigative methods usually employed in forgery cases are the same as in most criminal cases, i.e., obtaining complete details from all persons having knowledge of the incident, taking statements where necessary, evaluating information collected, narrowing the suspects, and interrogation. However, basic to the forgery investigation are several techniques, namely document examination, handwriting analysis and, fingerprint examination. These techniques are usually the principal ones used in the forgery case because they generally afford the best means for implementing a solution. It is not necessary for the agent to be an expert in these techniques, but he should be aware of the benefits to be obtained from their proper use.

b. Theft, forgery, alteration, etc., of U. S. Treasury checks will be thoroughly investigated. In those cases where a suspect is subject to the UCMJ, the NCIS will notify the USSS and conduct an investigation. Where the suspect is unknown or is not subject to the UCMJ, the USSS should also be apprised; concurrent investigations are encouraged. When requests for investigation are received outside the United States where there is no USSS present, NCIS may unilaterally conduct the entire investigation.

c. Generally, the following investigative steps are pertinent in the investigation of forgery:

(1) Develop evidence regarding an intent to defraud by setting out certain acts and circumstances leading to the act.

(2) Obtain from the person receiving the forged instrument a complete account of the circumstances at the time the instrument was passed.

(3) To whom was the forged instrument presented? Where and when was it presented? Obtain complete statements.

(4) Was the instrument presented in exchange for money or property? What was paid?

(5) Obtain the original forged instrument. If not available, obtain a copy.

(6) Fully identify the person whose name was forged and the name and location of the bank or institution through which the instrument passed. Obtain a statement from him disavowing the signature as a forgery.

(7) If the instrument passed through a bank, interview bank officials for any pertinent information. Were any similar forged checks received there?

(8) Obtain handwriting specimens from the payee and all suspects for comparison purposes.

(9) As appropriate, obtain finger and palm prints from suspect(s) and others for elimination purposes.

(10) Check appropriate criminal records to determine any previous record on suspects.

(11) Develop any evidence of direct or indirect gain to the forger as a result of the forged instrument.

(12) In cases of a false set of orders, discharge papers, birth certificates, notices of promotion, the basic questions are: did the individual whose name appears as a signature on the document actually prepare and sign it? If not, who did prepare and sign it? If the document was generated by a printer, what type of printer was used? Was alteration made under circumstances indicating genuineness or lack of genuineness?

24-14.9. Non-Sufficient Funds (NSF) Checks.

a. Another offense that is carried under the 4K and 4J subcategories involves making, drawing, or uttering a check, draft, or order without sufficient funds in violation of Article 123a, UCMJ. In this offense, the instrument is made, drawn, uttered, or delivered upon any bank or other depository, either:

(1) For the procurement of any article or thing of value, with intent to defraud; or

(2) For the payment of any past due obligations, or for any other purpose with intent to deceive, knowing at the time of the making, drawing, uttering or delivering that the maker or drawer has not or will not have sufficient funds in, or credit with, the bank or other depository for the payment of that instrument in full upon its presentment.

b. Precise legal definitions of the terms "uttering," "delivery," "article or thing of value," "past due obligation," "intent to defraud," and so forth may be found in paragraph 49c, Manual for Courts-Martial, U. S. 1984.

c. Proof in NSF Cases. When the instrument is given for the payment of a past due obligation or procurement of an article or thing of value:

(1) That the accused made, drew, uttered, or delivered a check, draft or order payable to a named person or organization, as alleged;

(2) That he did such act for the purpose or purported purpose of effecting the payment of past due obligation or of procuring an article or thing of value;

(3) That such act was committed with intent to defraud; and

(4) That at the time of making, drawing, uttering, or delivering of the instrument he knew that he or the maker or drawer had not or would not have sufficient funds in, or credit with, the bank or other depository for the payment thereof upon presentment.

d. Attention is invited to the fact that making, drawing, uttering, or delivery of a forged instrument are separate acts of the offense, i.e., separate persons could be involved with the making and drawing of the questioned instrument and yet another person or other persons could be involved in the uttering and/or delivery of the instrument. Conspiracy becomes a fact in this activity and must be considered in the investigative effort.

e. Investigative Policy and Procedures in NSF Check Cases.

(1) Statistical data maintained at NCISHQ indicates that in the past NCIS field components have responded to requests for NSF check investigations whereby in most cases the final investigation product was utilized merely to affect restitution from the offender. Therefore, it is NCIS policy not to accept for investigation any NSF check cases if the following offender status

exists at the time of the request:

(a) Active duty military members/or dependents.

(b) Retired members or dependents of the regular Navy, naval reserve, or fleet reserve.

(c) Inactive duty members of the naval reserve.

The responsible command has the resources and ability to take administrative or judicial action against the above offender groups without calling upon the investigative expertise of the NCIS. The appointing of an investigating officer or utilizing base investigators to cover the minimal logical investigative steps will provide the basis for the command to take appropriate action against the offender.

(2) NCIS will continue to accept for investigation those NSF check cases when face value of the check is more than $500.00 where:

(a) The military member/dependent continues to write NSF checks after closing the account.

(b) The military member is pending imminent discharge or is in a UA status.

(c) The military member opens a checking account with a minimum deposit and immediately commences to write a series of NSF checks against the account.

(d) The military status of the offender cannot be verified by the command.

(e) The military member/dependent claims non-authorship of the NSF check(s), no matter what face value.

(f) It is emphasized that the more than $100.00 face value applies to each check and not an aggregate of checks written by the offender.

(3) Investigation in NSF check cases will follow a logical line of inquiry designed to furnish the proof required, as set forth above. In general, the routine interview and interrogation techniques are indicated. Copies of bank records are especially important to show the state of the account, or lack of existence of one, as well as the fact of due notice of dishonor, or failure to give such notice, by the bank.

(4) It is important also to establish whether the suspect drawer or maker has subsequently made payment to the payee, and the exact date such payment, if any, was made. The suspect drawer or maker must make payment within five days of receipt of due notice of insufficient funds. If such payment is not made, a statutory rule of evidence may be applied to establish prima facie the knowledge of insufficient funds and the intent to deceive or defraud. Should the accused have made payment within the five-day period after receiving notice, or should he not have received

notice, these factors furnish no defense, but merely preclude the prosecution from availing itself of the statutory rule of evidence. The elements of knowledge and intent in such instance can still be proven by other means.

24-14.10. Obtaining Original U. S. Treasury Checks.

a. The U. S. Treasury Department will not release original Treasury checks to NCIS if the checks are for forgery cases within the United States. Therefore, all such requests for checks must be made through a local USSS Office.

b. Overseas, where there is no local USSS Office, U. S. Treasury checks must be obtained from the Check Information Section, Check Claims Branch, U. S. Treasury Department, Washington, D.C. Requests for checks by NCIS are to be centralized at the seat of government under the control of NCISFO Washington, D.C. All requests of checks, including those originated by USSS, are handled the same way by Treasury. Checks are usually not received for a period of several weeks to several months following the request. This is due to a huge volume of requests from many different federal, state, local, and foreign agencies; the millions of checks in storage; and bureaucratic vagaries. Experience has shown the process cannot be sped up appreciably by the subpoena process, by requests for expeditious handling based on speedy trial considerations, or by other measures short of a genuine, major emergency.

(1) When requesting U.S. Treasury checks from an overseas office, NCIS field components will send a lead to the NCISFO Washington, D.C. The NCIS field component will submit the following information: 1) Name of payee; 2) Symbol number (4 digits located in the far right hand corner of the check); and, 3) Serial number (8 digits located in the far right hand corner of the check near the symbol number). These items must be accurate in order to retrieve the check. NCISFO Washington, D.C. will request the check and will forward it to the requesting field component as soon as received. If a check cannot be located within 45 days of a request, Treasury will provide a status report to NCISFO Washington, D.C. If the check has not yet been negotiated, Treasury will so advise, and another request must be submitted later from the requesting NCIS field component.

(2) Treasury frequently can provide certified photocopies of checks in a much shorter period than it can provide the original checks. If such information will suffice, i.e., when all that is wanted is the identity of the clearing bank, considerable time can be saved by requesting only a copy of the check. Treasury prefers to provide original checks, but if an original is not available for some reason, a certified copy may be furnished. All original Treasury checks (forgery and non-forgery cases) acquired via NCISFO Washington, D.C. are to be returned to Treasury, via NCISFO Washington, D.C., as soon as possible after a case has been adjudicated, or when it is no longer needed as evidence. NCISFO Washington, D.C., then sends the check back to Treasury.

(3) Most investigations of this nature begin at the Base Disbursing Office with an individual claiming his government check is lost or stolen. This is where the initial processing takes place. When a check is first reported lost, stolen or not received, the Disbursing Office immediately places a stop payment on the check and obtains a statement from the claimant. The stop payment acts as a signal that allows Treasury to expeditiously identify forgeries. Later, if a forgery has taken

place, Treasury will send its own claims form for the claimant to fill out. Treasury will not release the original check to NCIS until this completed form has been returned. This step becomes very important because some claimants, particularly those who have already received a substitute check (or persons who cashed both checks) are in no hurry to complete the form. Delays of up to 180 days in check retrieval have been attributed to claimants not promptly completing the form. Therefore, NCIS agents should ensure that Treasury claim forms are promptly submitted by the payee.

(4) Registered U. S. Mail is to be utilized for shipment of Treasury checks by NCIS components. For documentation and tracking purposes, the sending office will notify the receiving office of the shipment to include contents, shipment date, and tracking number. . Treasury treats these checks as self-authenticating and sends original checks to NCIS without chain of custody. The field component will follow current guidelines regarding evidence custody control of the checks during the investigative and adjudication stages. When the check is no longer required for investigation or adjudication, it shall be properly disposed from the evidence controls and returned (via Registered Mail) to NCISFO Washington, D.C. for return to Treasury.

24-14.11. Investigations Of Treasury Check Forgeries In The Western Pacific. Treasury occasionally requests NCIS investigative assistance in areas where there is no USSS support. NCIS will accept requests from Treasury regarding forgery of checks cashed in Western Pacific (including the Philippines and Hong Kong) only when the payee address on the face of the check is an FPO address and the payee is a person under U.S. jurisdiction or in whom the U.S. has other significant interest. Exceptions may be made whereby NCIS will accept for investigation those incidents involving large amount alteration or other unique circumstances.

24-15. SUBCONTRACTOR KICKBACKS (SUBCATEGORY 4L).

24-15.1. When a subcontractor makes any payments, fees, commissions, credits, gifts, gratuities, or compensations of any kind to prime or to higher tier contractors or to any officers, partners, employees, or agents of higher tier subcontractor or prime contractors, the act constitutes a form of commercial bribery known as a subcontractor kickback.

24-15.2. The detection of this practice may require extremely meticulous investigation and an intimate familiarity with local business procedures because illegal kickbacks are readily concealable, commonplace in all phases of defense contracting and can easily be contrived within the commercial structure. In any such activity, the government becomes the recipient of inflated costs. Further, the integrity of the federal acquisition process is compromised and the subcontractor's performance may be well below the prescribed norm, owing to the amount of the kickback.

24-15.3. The Federal Anti-Kickback Act, 41 USC 51-54 as amended 7 November 1986 by Public Law 99-634, the Anti-Kickback Enforcement Act, is similar in purpose to the bribery statute, 18 USC 201, and is construed under the same principles. A criminal act is constituted by the offer of a kickback in the form of anything of value and applies as well to persons who solicit, accept, or attempt to accept kickbacks. Criminal penalties under the law include a prison term up to ten (10) years and compensation to the government of twice the amount of each kickback plus a $10,000 fine for each kickback payment. The law further requires contractors to establish internal programs to detect and prevent kickback activity, to report such violations to the DODIG and to cooperate fully

in any kickback investigations. The law also authorizes the DODIG access to a contractor's facilities and records to determine compliance with the anti-kickback statutes.

24-15.4. A violation of the Anti-Kickback Act rarely occurs without a collateral offense. Persons involved in any form of commercial bribery may also be in violation of one or more of the following:

a. 18 USC 286, Conspiracy to defraud the government with respect to claims; 18 USC 287, False, Fictitious or Fraudulent Claims;

b. 18 USC 371, Conspiracy to Commit Offense or to Defraud the United States; and 18 USC 1001, False Statements.

24-15.5. The Subcontractor Kickbacks section of the Federal Acquisition Regulation (FAR 3.502) bases its authority in the Anti-Kickback Act and dictates that agencies shall report suspected violations of the Act in accordance with agency procedures.

24-15.6. Kickback schemes are among the oldest dishonorable business practices and among the simplest to incorporate within the contracting tiers. They prove extremely costly to the government because their illegal profits may be distributed as far as the lowest levels of production.

24-16. COST MISCHARGING (SUBCATEGORY 4M).

24-16.l. When a contractor charges or attempts to charge the government for costs which are not allowable, not reasonable, or which cannot be either directly or indirectly allocated to the contract, cost mischarging exists.

24-16.2. The Federal Acquisition Regulation (FAR 31.201, 31.202, 31.203, and 31.205) outlines the four factors to be considered as cost principles:

a. Reasonableness. The cost may not exceed that which would be incurred by a reasonable competitive businessperson in the conduct of competitive business.

b. Allocability. A connection must be shown between the contract and its particular cost to ensure that the government does not pay for costs primarily to the contractor's benefit.

c. Limitations and Exclusions. These are determined by negotiation, are governed by the FAR, and vary with individual contracts. The contractor's ability to charge the government for specific items of costs may be limited, negated, or allowed, depending upon its particular nature and its relationship to government objectives.

d. Cost Accounting Standards - A contractor is responsible to the government for conducting business, including record keeping, in a manner that facilitates government auditing. Allowable costs to the government may not be misrepresented, concealed, or represented on alternate accounts.

24-16.3. All allowable costs, either direct or indirect, are reimbursable and identified in the FAR. A

contractor who claims compensation for indirect costs must include in his proposal for settlement, a certification that all indirect costs involved in the transaction are allowable.

a. Certain unallowable costs in government contracting, as defined by 10 USC 2324, include, but are not limited to:

(1) Costs of entertainment, including amusement, diversion, and social activities, and any costs directly associated with such costs (such as tickets to shows or sports events, meals, lodging, rentals, transportation, and gratuities).

(2) Costs incurred to influence (directly or indirectly) legislative action on any matter pending before Congress or a state legislature.

(3) Costs incurred in defense of any civil or criminal fraud proceeding or similar proceeding (including filing of any false certification) brought by the United States, where the contractor is found liable or has pleaded nolo contendere to a charge of fraud or similar proceeding (including filing of a false certification).

(4) Payments of fines and penalties resulting from violations of, or failure to comply with, federal, state, local, or foreign laws and regulations, except when incurred as a result of compliance with specific terms and conditions of the contract or specific written instructions from the contracting officer authorizing in advance such payments in accordance with applicable regulations of the Secretary of Defense.

(5) Costs of membership in any social, dining, or country club or organization.

(6) Costs of alcoholic beverages.

(7) Contributions or donations, regardless of the recipient.

(8) Costs of advertising designed to promote the contractor or its products.

(9) Costs of promotional items and memorabilia, including models, gifts, and souvenirs.

(10) Costs for travel by commercial aircraft which exceed the amount of the standard commercial fare.

b. Authority to allow reimbursement for costs not prescribed by directive rests solely with the Secretary of Defense.

24-16.4. The three common types of cost mischarging are:

a. Accounting Mischarging. This scheme may include a contractor knowingly charging unallowable costs to the government, concealing or misrepresenting them as allowable costs, or hiding them in other accounts.

b. Material Cost Mischarging. This may take the form of inflated raw material cost, falsification of accountability records, concealed theft of government-owned materials, or improper billing.

c. Labor Mischarging.

(1) In a transfer of labor cost, a contractor will attempt to eliminate a monetary loss on one contract (usually a firm fixed price) by transferring the labor cost to another contract (usually a cost type contract). The contractor may claim that his transfer of labor costs was made to correct an error in his accounting process.

(2) In an erroneous time and charges scheme, the contractor attempts to charge the government for labor hours that were not actually expended. This type of fraud may be detected by comparing the contractor's labor distribution and time cards with the contractor's actual charges for work performance.

(3) A contractor may destroy original time cards and replace them with fraudulent ones. He may also alter, or cause to have altered, any time cards or work logs in order to fabricate the amount of hours spent on a contract.

(4) A contractor may falsify costs of general and administrative expenses, overhead, security, storage, packing, and packaging or shipping.

24-16.5. Cost mischarging invariably results in increased costs to government. Applicable statutes include 18 USC 286, Conspiracy to Defraud the Government with Respect to Claims; 18 USC 287, False, Fictitious or Fraudulent Claims; 18 USC 1001, False Statements.

24-17. ENVIRONMENTAL CRIMES (SUBCATEGORY 4N).

24-17.1. This subcategory pertains to the reporting of matters regarding the unlawful storage, transportation, or disposal of hazardous waste or toxic pollutants. Violators can be companies or individuals (military, civilian or contractor). Under various circumstances, actions by DON employees and/or contractors can cause the DON to be civilly liable for their violations of environmental laws.

24-17.2. Jurisdiction over environmental crimes rests with the Environmental Protection Agency (EPA), the FBI, and where there is DON interest, NCIS. Numerous statutes and regulations pertain, including the Federal Water Pollution Control Act or Clean Water Act (33 USC 1251-1376), the Clean Air Act (42 USC 7401-7642), the Toxic Substances Control Act (15 USC 2601-54), the Comprehensive Environmental Response, Compensation and Liability Act (42 USC 9601-9675), the Resource Conservation and Recovery Act (42 USC 6901-87), OPNAVINST 5090.1B (Environmental and Natural Resources Protection Manual), and various articles of the UCMJ to include 92, 107, 108, and 134. In addition, there is a wide range of state laws that may be applicable to individual investigations with equally wide ranging criminal and civil penalties.

24-17.3. Generally, there are two main categories of persons who violate the statutes. First are

those persons who try to operate outside the system. These persons clearly deal with toxic or hazardous substances, but attempt to dispose of them without notifying the government, thereby saving enormous sums in legal compliance costs. Discharging or disposing materials without a permit are fundamental criminal offenses. These offenders can be either businessmen or "midnight dumpers" who dispose of their businesses' waste for profit. The second main category is composed of those who do operate within the regulatory system, but who undermine the regulatory scheme by materially misrepresenting or concealing the extent of toxic substances or pollutants with which they deal, often with violations of the False Statements Act (18 USC 1001). In both cases, knowing violations can create costly undisclosed hazards to health and the environment.

24-17.4. Standard steps to be taken when investigating environmental crimes may include evidence collection, laboratory analysis of evidence, surveillance, searches, interviews, and records and contract reviews to determine such things as whether or not the government has been billed for proper disposal costs when in fact the substances were unlawfully disposed.

24-17.5. Prosecutors will focus on several key factors. The first concerns evidence of knowledge or intent. Mistakes made in honest corporate compliance efforts are not criminal; but operating policies that encourage cutting corners, fail to meet government standards, and shield managers from the facts clearly can produce criminal liability. Other factors that prosecutors look for include the harm that flows from the violation, the economic gain to the violator as a result of the violation, and whether the violations were aggravated or extensively repeated. Actions to conceal or mislead the government, along with a substantive violation of pollution laws, make criminal prosecution more likely.

24-18. PRODUCT SUBSTITUTION (SUBCATEGORY 4P).

24-18.1. When a contractor delivers, or attempts to deliver, to the government goods or services which do not conform to contract requirements, without informing the government of the deficiency, while seeking reimbursement based on the delivery of conforming products or services, is known as Product Substitution. This aspect of fraud includes, but is not limited to:

a. The provision of inferior quality raw materials.

b. A contractor's failure to test materials as specified in the contract.

c. Providing foreign-made products when domestic products were required.

d. Utilizing untrained workers when and where skilled technicians were required.

24-18.2. If a contract requires the delivery of an item produced by the original equipment manufacturer (OEM), no substitute is authorized. When a contract demands the delivery of end items produced in the United States, no deviations from the requirement are acceptable. If the contract specifies exact test requirements for a product, they must be conducted within contractual parameters.

24-18.3. No contracting province is immune to the possibility of product substitution because its

likelihood is as limited as the amount of available goods and services. The following variables are conducive to creating the climate for this type of fraud:

a. A history of poor performance by a contractor.

b. A negative pre-award survey.

c. An award to an unusually low bidder.

d. Inadequate government inspection and testing.

e. Over-reliance on the contractor's documentation.

f. Misuse of "fast pay" contracts (“fast pay” contracts are defined in FAR 52.213.1 and allow for an expeditious payment to the contractor).

24-18.4. Product substitution is one of the most critical aspects of fraud because:

a. A substitute for any product or service is almost never as good as the item specified in the contract.

b. A substitute undermines the reliability of the entire Defense Supply System.

c. A substitute damages the integrity of the competitive procurement system.

24-18.5. Product substitution can be applied to any medium, from tooling to fabrics to fungible goods to components of major weapons systems - in short, to anything for which the government contracts. Whenever there is suspected product substitution, NCIS field components are reminded of the requirement that the affected systems command and the NAVSUP be promptly notified. Such notification is necessary to perform an evaluation of the effect on mission readiness and to address safety issues involved. Applicable statues include 41 USC 10, Buy American Act; 18 USC 287, False, Fictitious or Fraudulent Claims; and 18 USC 1001, False Statements or Entries Generally.

24-19. FRAUD INVESTIGATIVE SURVEY (SUBCATEGORY 4S).

24-19.1. This subcategory is used for an in-depth probe of a specific operation, activity, or program to determine if the systems being utilized are susceptible to criminal exploitation and if exploitation is present. The survey is not designed to take the place of investigations into known or suspected irregularities, but to scrutinize existing operations, activities, or programs to ensure compliance with government requirements and directives. Such surveys may be conducted within, but are not limited to:

a. Small/disadvantaged business concerns.

b. Application of labor laws to government acquisition.

c. Environmental, conservation, and occupational safety.

d. Foreign acquisition.

e. Foreign military sales.

f. Government-furnished property and materials.

g. Quality assurance.

h. Acquisition/Disposition cycles of material.

i. Pay and Allowance, including overtime.

24-19.2. Planning The Survey. Fraud Investigative Surveys should be well planned, thoroughly researched, and appropriate references studied prior to initiating the actual survey. The planning and research should provide the first indication of the specific areas anticipated during the survey. The team leader should collect and review pervious surveys, Naval audit reports, and other reports of investigations that may be available. The team leader should also obtain and review all applicable references on the activity to be surveyed. A pre-survey site visit must be accomplished within one week of case initiation. A ROI should be prepared reporting the results of the site visit and requesting any technical support that may be required.

24-19.3. Conduct Of Surveys.

a. Normal investigative techniques should generally be applied during the conduct of a survey, as a survey can best be described as an investigation with the object of identifying criminal acts, crime-conducive conditions, and persons engaging in criminal activity.

b. Specific criminal acts detected during the course of a survey should normally be referred to the NCISRA servicing the activity.

c. The use of cooperating witnesses prior to and during the survey can provide beneficial information pertaining to the operation of the facility. Continuous effort should be made to develop reliable sources of information within those facilities subject to surveys.

24-19.4. Reporting Requirements.

a. No set format is established for reporting the findings of Fraud Investigative Surveys, and each ROI will necessarily be tailored to meet the reporting requirement of the specific survey. However, all surveys share common areas of interest, and, as such, the following general areas of information will be included in all 4S ROIs:

(1) Identity of function/activity surveyed.

(2) Introduction/background on the nature and universe of the area surveyed.

(3) Scope of the actual survey coverage.

(4) Summary of results.

(5) Discussion section covering each type of substantive fraud conducive conditions noted to include:

(a) Description of condition;

(b) Extent of vulnerability;

(c) Examples as needed to illustrate condition (each detailed step taken in identifying the condition is not necessary.); and

(d) Whether or not investigative referrals were made.

b. In addition, to facilitate the extraction of information, the following headings will be included in all 4S ROIs:

(1) Deficiencies. List crime conducive conditions or noncompliance with regulatory guidance, departure from lawful general orders or obvious violations, applicable statutes, laws, or prescribed standards, and an explanation of how a violation constitutes a crime conducive condition; if it is not self-evident from listing, that should be provided as well as the regulation, order statute, etc., violated.

(2) Discrepancies. Same as paragraph (1) above.

(3) Observations. List existing or potential crime-conducive conditions wherein an apparent violation of prescribed regulation does not exist. An explanation of how the observation is crime conducive should be provided.

(4) Criminal Investigations Initiated. When an investigation is initiated from a Fraud Investigative Survey, the CCN and the deficiency or observation related to the investigation should be listed if applicable.

24-19.5. NCISHQ approval is required prior to initiating any efforts under this case subcategory.

24-20. UNAUTHORIZED SERVICES (GOVERNMENT) (SUBCATEGORY 4T).

24-20.1. Investigations concerning fraudulently obtained services or unauthorized purchases and fraudulent use of U. S. Government credit cards (not involving forgery) or other charge accounts including U. S. Government telephone calling cards and Standard Form 44 are conducted under subcategory 4T where the victim is the government.

24-20.2. Evidence in subcategory 4T cases includes any relevant documentation executed by the

perpetrator or documentation which otherwise tends to substantiate the wrong-doing; demonstration of a tie-in between the perpetrator and the goods or services which were illicitly gained; interviews of witnesses, e.g., those who conducted transactions with, or received telephone calls from the perpetrator; interrogation; handwriting and/or fingerprint analysis.

24-20.3. Investigations of U. S. Government telephone calling card fraud or unlawful use of a government telephone must only be undertaken when significant government interest exists, i.e., felony criteria. A more complete discussion of telephone calling card fraud is found under Section 24-6, Credit Card Fraud.

24-20.4. Proper concern in unauthorized services cases must be exercised to preclude expenditure of NCIS investigative effort where significant government interest does not exist. In particular, NCIS will not serve in a bill-collecting capacity for commands.

24-20.5. Upon initiation of a fuel-related investigation (generally reported under the 4T case category), the ROI (OPEN) will include 23A in the info line. Code 23A will be responsible to inform the Defense Energy Support Center (DESC) Fuel Fraud Attorney of the investigation and provide an updated status during the course of the investigation.

24-21. TRICARE CLAIMS VIOLATIONS (SUBCATEGORY 4U).

24-21.1. TRICARE is the DOD program for providing medical and dental care to DOD active duty members in locations where military treatment facilities are not available or are unable to provide the required care. Due to the proliferation of outsourcing logistical services within the DOD, the use of TRICARE services is common even in areas with large military treatment facilities. DOD Directive 5136.12, TRICARE Management Activity, dated 31 May 01, established the TRICARE Management Activity (TMA) as the controlling authority for all issues pertaining to fraud within the TRICARE program. As mentioned in Paragraph 24-4.2.b.(2), DCIS has primary jurisdiction of all investigations involving fraud by healthcare providers associated with TRICARE. NCIS Special Agents should notify DCIS of all investigations that indicate collusion or involvement by health care providers.

24-21.2. Suspected TRICARE fraud will be investigated under suspected violations of Articles 107 (False official statements) and 132 (Frauds against the U.S. Government) for persons under the jurisdiction of the UCMJ and suspected violations of 18 USC 287 (False claims), 18 USC 1001 (False statements), and/or 18 USC 1341 (Mail fraud) for those under federal jurisdiction.

24-21.3. The TMA Program is responsible for initiating administrative action to recoup losses associated with TRICARE fraud. This is done by the TMA Program Integrity Office (PIO) under the authority of the Debt Collection Improvement Act of 1996. The PIO has the authority to recover lost funds, suspend or terminate relationships with TRICARE providers who are found to be involved in fraudulent activities. Lost funds can be recovered from DON active duty members via administrative action by the command.

24-22. WORKERS COMPENSATION (SUBCATEGORY 4W). The Federal Employees Compensation Act (5 USC 8101) sets forth procedures whereby civilian employees of the

government (as defined by the Act) may receive compensation and medical care for job related injuries and disability growing there from. Compensation is paid based on a claim filed by the employee; thus, fraud is normally prosecuted under the False Statement or Fraud to Obtain Federal Employees' Compensation (18 USC 1920), Federal False Claims Statute (18 USC 287) and False Statements Statute (18 USC 1001).

a. Elements of Proof (False Claims):

(1) The existence of a claim, which may be either a demand for money or the transfer of public property;

(2) That the claim was presented to the U.S. Government;

(3) That the claim contains a false statement of fact;

(4) That the suspect had knowledge that the claim was false and with such knowledge intentionally submitted the claim.

b. Elements of Proof (False Statements):

(1) That the suspect knowingly made a false statement;

(2) Which was material (i.e., having the natural tendency to influence, or be capable of affecting or influencing, a government function);

(3) And the statement was made with regard to any matter within the jurisdiction of any agency or department of the United States.

c. Investigations into suspected fraudulent injury/disability claims are often worked concurrently with agents of the U. S. Department of Labor (DOL), Office of Worker's Compensation Programs (OWCP). OWCP administers the Employees Compensation Act and payments to disabled personnel are made by the DOL. The DON is the victim of disability claims fraud by covered civilian employees of the Navy and Marine Corps. This is true because the DON must repay the DOL annually for monies paid in compensation to naval civilian employees.

24-23. INTEGRATED SUPPORT (SUBCATEGORY 4Y).

a. The Integrated Support Special Operations is the primary document to be utilized to report integrated agents' activities within the command. The initiation of the 4YSO will be documented via ROI (OPEN). The title of the 4YSO will identify the command followed by "Integrated Fraud Support to Command." The "Narrative" section of the ROI (OPEN) will, at a minimum, address the following:

(1) Brief description of the command, its mission and responsibilities, AOR, parent subordinate commands, off-site facilities.

(2) Identify key command and contracting personnel.

(3) Identify the major procurement programs, to include the total dollar value of the program, annual expenditures, current status, prime and sub-contractors, and any vulnerabilities identified.

(4) In conjunction with the command, prioritize their major procurement programs. Based on these priorities, the integrated agent will be responsible for identifying those programs most susceptible to fraud, waste and abuse, and having those particular programs reviewed and analyzed for various indicators of fraud. The integrated agent is not expected to be a contract specialist or analyst, and therefore should not be expected to review and analyze the voluminous contracts themselves.

(5) Brief synopsis of goals and objectives for the first 60-day period.

b. An ROI (INTERIM) will be generated every 60 days during the pendency of the 4YSO. Any investigation initiated as a result of the operation will be referenced and a brief description will be set forth in the "Executive Summary" paragraph of the report. All criminal intelligence reports generated during the reporting period will also be referenced in that section of the report. (NOTE: All investigations generated based on intelligence developed by the integrated agent must reference the criminal intelligence report as predication. Likewise, the integrated agent must reference the ROI (OPEN) investigation on the 4YSO Interim report). The "Narrative" section of the report will, at a minimum, address the following:

(1) Provide a brief description of all criminal information reports and investigations initiated during this reporting period;

(2) Discuss the major procurement programs identified in the ROI (OPEN), to include their status in the procurement process, dollar values (may involve multiple, related contracts), the number of programs reviewed, the number of contracts reviewed, vulnerabilities identified, liaison, and the impact to the command;

(3) Key contractors (prime and sub-contractors), locations involved, contracts awarded, and dollar values;

(4) Meetings conducted with the command (staff meetings, task force meetings, etc.);

(5) Liaison with the Navy Acquisition Integrity Office, NAVAUD SVC, DCAA, DCMA, U.S. Attorney's Office, or other DOD or law enforcement organizations;

(b)(7)(E)

c. The “Narrative” paragraph should also be used by the integrated agent as an opportunity to describe the key events and economic crime support provided to the command during this reporting period.

d. General information developed during the course of the 4YSO must be reported via an IA and attached as an exhibit to a criminal intelligence report, ROI (INFO). This includes interviews of command/contract personnel who provide information germane to the command (i.e., infrastructure, organizational charts, priority systems within the command, command or system vulnerabilities), RTP systems intelligence, possible fraudulent activity within the procurement process, other criminal intelligence (i.e., narcotics, theft), CI/CT/FP information, administrative anomalies, security weaknesses and any other actionable information which should be brought to the attention of the command for possible corrections or improvements. The ROI (INFO) report will be referenced on the appropriate 4YSO.

24-24. LOSS/RECOVERY VALUE. The Inspector General Act of 1978 levied a requirement to report dollar recovery values or losses sustained of government funds and property as determined during certain types of investigation conducted by government investigative agencies. These reports are provided to Congress and also made public. To facilitate the extraction of this required information from NCIS fraud investigations, the dollar value will be reported as soon as known, preferably in the ROI (OPEN). It will also be reflected under a separate heading entitled, "LOSS/RECOVERY VALUE" in the closing ROI. The dollar values must accurately reflect actual figures as determined by command authority. When this cannot be obtained, an estimate must be provided.

24-25. QUI TAM ACTIONS.

24-25.1. The False Claims Act, originally enacted in 1963, allows a person or organization with knowledge of an alleged fraud committed against the U.S. Government to file a civil suit, on behalf of the U.S. Government, against the person or organization allegedly committing fraud. These complaints are called Qui Tam (pronounced KEE-TAM) which is derived from the Latin “Qui tam pro domino rege quam pro sic ipso in hoc parte sequitur” meaning “who as well for the king as for himself sues in this matter.” The person who files the claim, called a relator, does not have to have been harmed by the fraudulent activities. The relator benefits for reporting the information by receiving a portion of the monetary recoveries resulting from the complaint, plus legal costs. Given the high value of many U.S. government contracts, the relator stands to receive a sizeable award from a successful Qui Tam complaint.

a. The Qui Tam action must be based on information not known to the U.S. Government at the time of its filing. Once the action has been filed, the U.S. Government has 60 days to investigate the allegations and, if deemed accurate, assume control of the investigation. NCIS personnel involved in Qui Tam investigations will follow normal NCIS procedures in regard to all aspects of the investigation with the exception of dissemination of information outside of NCIS.

b. The following information cannot be released outside of NCIS without prior approval of the Department of Justice:

(1) The fact that a Qui Tam action has been filed,

(2) The identity of the relator in the Qui Tam action, and

(3) Disclosure of the allegation(s) to the defendant(s).

c. DOD Instruction 5240.4, Reporting of Counterintelligence and Criminal Violations, dated 22Sep92, requires that NCIS inform the DOD and DON leadership of all "significant" investigations. In the case of Qui Tam actions, only the circumstances of the allegation will be provided. The fact that a Qui Tam action has been filed and the name of the relator will not be released. The definitions for "significant" investigations include:

(1) A potential loss to the U.S. Government of $500,000 or more,

(2) Corruption of a public official, regardless of the monetary loss,

(3) Suspected misconduct involving an O-6 or GS/GM-15 and above with a potential loss of $5,000 and above,

(4) Serious hazard to health or safety, or operational readiness, regardless of loss value,

(5) Suspected misconduct involving a Commanding Officer or Officer-in-Charge.

d. As mentioned in Paragraph 24-4.2.b.(3), SECNAVINST 5430.92B, Assignment of Responsibilities to Counteract Fraud, Waste and Related Improprieties Within the Department of the Navy, requires NCIS to inform specific DON components of all investigations pertaining to acquisition fraud and environmental crimes. The instruction allows for exceptions to include Qui Tam investigations.

e. All reporting containing Qui Tam information should include the following caveat at the top of the report:

QUI TAM: EXISTENCE OF THE QUI TAM SUIT AND IDENTITY OF THE RELATOR MUST NOT BE DISCLOSED WHILE THE QUI TAM IS UNDER SEAL. SPECIFIC DETAILS OF THE QUI TAM ALLEGATION SHOULD NOT BE BRIEFED OUTSIDE OF THE NAVAL CRIMINAL INVESTIGATIVE SERVICE WITHOUT AUTHORIZATION FROM THE DEPARTMENT OF JUSTICE.

f. Ammendments to the False Claims Act also include what is now commonly referred to as "Whistleblowers Protection" to encourage people with knowledge of fraudulent activities to come forward.

24.25-2. The DOD established the Voluntary Disclosure Program in 1986 to provide a means by which contractors working with the DOD could report suspected fraudulent activities among other DOD contractors. This program allows for monetary awards to contractors who report fraudulent

activities although the value of the awards is limited to $10,000 or 1% of the total savings to the DOD, whichever is less. Specific details of this program can be found in DOD Directive 7050.4, Awards for Cost Savings Resulting form the Disclosure of Fraud, Waste or Mismanagement, dated 21Oct04.

24-26. DOD INSPECTOR GENERAL SUBPOENAS.

24-26.1. The DOD Inspector General (DOD/IG) was granted administrative subpoena authority by the Inspector General Act of 1978. NCIS is able to utilize DOD/IG administrative subpoenas when conducting an investigation that is in furtherance of a function of the DOD/IG. Since investigations involving acquisition fraud, bribery, conflict of interest, and other such activities are clearly functions of the DOD/IG, their subpoena authority is available to NCIS during the conduct of these investigations. When NCIS utilizes a DOD/IG subpoena during the course of an investigation, it in effect is conducting the investigation for DOD/IG.

24-26.2. The main benefit of using the DOD/IG subpoena is that the information obtained is not restricted in the same manner as with grand jury subpoenas. Unlike information obtained via a grand jury subpoena, information obtained from DOD/IG subpoenas can be disclosed to a broader audience, civil and/or administrative proceedings, and during contractual remedies. Also, the use of a DOD/IG subpoena provides a U.S. Attorney the ability to obtain and review documents prior to compelling grand jury testimony.

24-26.3. The DOD/IG subpoena power is limited to issuing "Subpoenas Duces Tecum" – subpoenas that require the receiver to produce already existing documents. The DOD/IG subpoena cannot be used to compel testimony. Also, the DOD/IG subpoena itself does not carry punitive measures for non-compliance. In the case of non-compliance, the DOD/IG must petition a U.S. District Court to order compliance, in which case non-compliance would be punished as contempt.

24-26.4. The DOD/IG subpoena is generally used to obtain information in one of four categories:

a. Business Records: A DOD/IG may require production of business records from businesses and subcontractors.

b. Personal Records: An individual may be required to produce personal records such as bank statements, employment records, and personnel records of a company employee.

c. Financial Records: Financial institutions may be required to produce records of its customers. However, the Right to Financial Privacy Act of 1978 requires financial institutions to notify customers that their records have been released pursuant to a DOD/IG subpoena either prior to release or at the time of the release if the customer is an individual or a partnership of five or less individuals. This requirement does not apply to corporations, business trusts, or partnerships of six or more individuals. Also, the Act has clauses that allow for a delayed notification in the event that secrecy or surprise is essential to the investigation.

d. Government Records: The DOD/IG subpoena may be used to obtain desired documents from state and local agencies but not from other U.S. Government agencies.

24-26.5. The DOD/IG subpoena should not be used to obtain information that is obtainable through less stringent methods and investigative techniques. For example, many contracts are written with an "audit clause" that allows DOD auditors to obtain all records pertaining to the contract at any time. The party receiving a DOD/IG subpoena may challenge it in court by showing that the information could have been obtained via normal procedures.

24-26.6. Although the DOD/IG subpoena cannot compel a person to testify, it can compel the recipient to provide testimony regarding the accuracy and authenticity of the documents provided. Special Agents must remember to limit the scope of their questions to this subject and, if further testimony/statements are desired, advise the recipient that those questions are outside of the verification process, and he/she is not compelled to provide further statements. Unless this distinction is made clearly and fully understood by the recipient, any statements provided may be ruled inadmissible during subsequent judicial proceedings.

24-26.7. The DOD/IG website, http://www.dodig.mil/Inspections/IPO/Subpoena/SubpoenaIndex.htm, contains guidance and the forms required to request a DOD/IG subpoena, as well as sample documents. As outlined on this website, requests for a DOD/IG subpoena can be sent directly from field offices to the DOD/IG via e-mail. The senior NCIS representative to the DOD/IG should be included on all requests as a courtesy copy. The DOD/IG website provides contact information for the DOD/IG Subpoena Program Manager and encourages personnel requesting a DOD/IG subpoena to discuss their needs and the specific wording of their subpoena requests prior to submission. The DOD/IG makes every attempt to process subpoena requests in a timely manner. Since incomplete or incorrect requests add delays to the processing time, communications with the Subpoena Program Manager prior to the submission of a request are encouraged.

CHAPTER 25
TITLE: BOMB & ARSON (CATEGORY 6A)
POC: CODE 23A
DATE: AUG 07

25-1. GENERAL. This subcategory includes cases referred to NCIS in which arson and/or the use of an explosive device is suspected. Investigations of this nature include the suspected arson of government or private property including vehicles, aircraft, watercraft, buildings, or any property of value. Further, this subcategory includes investigations of suspected arson of wildlands (e.g., timber, brush, grass), and explosions which result in fire. Attempts and conspiracies to commit any of the above will also be investigated under this subcategory. All situations involving the receipt of a telephonic, electronic or mail threat, where no explosive device, real or hoax, is involved will continue to be reported under category 7B (Bomb Threat). The guidance and procedures that follow will obviously not be applicable or practical in all bomb and arson investigations. The special agent must recognize the complexity of an investigative situation, obtain assistance as required, and be flexible, persistent, and resourceful in order to conduct a thorough and professional investigation.

25-2. ELEMENTS OF ARSON.

25-2.1. There are two degrees of the crime of arson under the Uniform Code of Military Justice (UCMJ); simple arson and aggravated arson.

25-2.2. Simple arson elements are:

a. The accused set fire to or burned certain property of another;

b. The property was of some value;

c. The act was willful and malicious.

25-2.3. The willful and malicious intent element is often times the most difficult to establish and will be discussed in detail later in this chapter. Burning must be an actual burning or charring; a scorching or discoloration is insufficient to complete the offense. Burning may be defined as a change in the molecular structure of a material brought about by the application of heat. The identification of the suspect(s) as the culpable party is a self-explanatory element. That the

property is of some value and belongs to another is usually self-evident, but raises some related questions. A person cannot commit simple arson by setting fire to his own property; however, such incidents may involve fraudulent insurance claims or claims against the government, and should be investigated under this subcategory.

25-2.4. The value of the property burned has significance as the MCM provides for a maximum punishment of one year confinement if the value of the property is $500 or less. Such a crime is a minor offense and is therefore not within the jurisdiction of NCIS. However, if the potential for greater harm exists in such a situation (such as, a series of minor fires has been experienced, or a minor fire occurs under circumstances endangering more valuable property or human life, or operational capabilities are affected), an investigation should be conducted by NCIS. Arson in which the property value is greater than $500 is a major offense and within NCIS jurisdiction.

25-2.5. Aggravated Arson elements are:

a. Structure.

(1) The accused burned or set fire to a structure

(2) The act was willful and malicious;

(3) There was a human being in the structure at the time;

(4) The accused knew there was a human being other than the accused or his confederates at the time;

b. Inhabited Dwelling.

(1) The accused burned or set fire to an inhabited dwelling of another;

(2) The act was willful and malicious.

25-2.6. In the crime of aggravated arson, value or ownership of the burned property is immaterial. A person may be guilty of aggravated arson even against his own dwelling, whether owner or tenant. Aggravated arson may be committed by the burning of any building, vehicle, or shelter (including a tent), either public or private, movable or immovable, where the offender reasonably believes it to be occupied by a human being. It may be inferred that the offender has such knowledge when the nature of the structure, as a Navy Exchange Store or theater during hours of business, are shown to have been such that a reasonable man must have known of the presence of human beings therein at the time. The actual presence of a human being in an inhabited dwelling at the time of the burning is not necessary to constitute the offense of aggravated arson. An inhabited dwelling also includes the outbuildings that form part of the cluster of buildings used as a residence. A naval vessel qualifies as a structure with regard to the elements of aggravated arson.

25-2.7. Shipboard arson fires involving U. S. Navy vessels fall under the unique responsibility

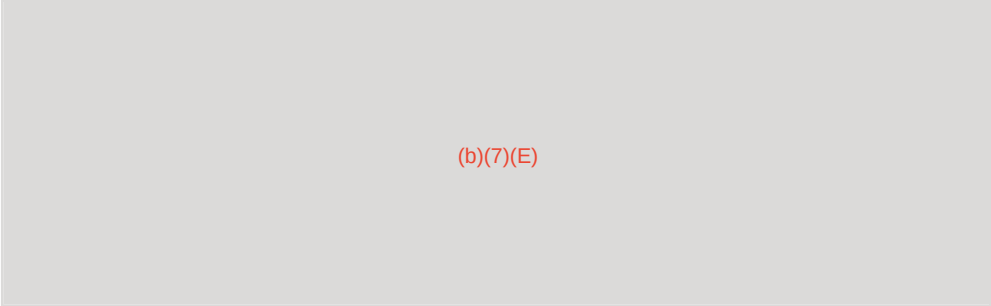
of NCIS. The investigating agent will be tasked with determining whether or not the fire was intentionally set (arson).

a. Welding/hotwork, electrical, mechanical, and other accidental causes must be evaluated/eliminated as the heat source of the fire. The use of cognizant shipboard personnel can assist greatly regarding this issue. If the fire is determined to be arson, the following guidance is provided:

(1) Shipboard arson fires most often occur as the result of two specific motivations:

(a) Revenge (approximately 80%); and

(b) Excitement/recognition (Hero Syndrome - 20%)



(3) Commonly, shipboard fires are started at or near the fire-starter's work center or berthing compartment.

b. Physical evidence in a shipboard fire which occurs while the vessel is operational may, by necessity, have been destroyed or eliminated. In cases involving shipboard fires, the primary concern of the ship's company is to extinguish the fire and prevent a reflash, further shipboard damage, and injuries. With this concern in mind, commands tend to dispose of burned materials and possible evidence by washing it overboard. Because of this necessity, it is essential that the responding agents immediately identify all members of the damage control and fire fighting parties and seal the spaces in which the fire occurred prior to the initiation of any repairs. All such personnel should immediately be questioned and the spaces examined. Ship's photographers or crew members who may have photographed the fire scene or the fire while it was in progress should be identified and their film obtained for examination.

25-2.8. Wildland fires are an offense under Title 18 USC 1855, punishable by fine and/or imprisonment not exceeding five years, when there is:

a. The accused, willfully and without authority;

b. Sets on fire;

c. Timber, underbrush, grass, or other inflammable material;

d. Upon the public domain or United States Government property.

25-2.9. It should be noted that in order to complete this offense there need not be a malicious intent, nor must there be property of value burned.

25-2.10. Explosions resulting from a fire will be investigated as a resultant act of the fire. Fires resulting from an explosion will be investigated under this subcategory, but will be investigated as an explosion vice a fire. Associated categories of wrongful destruction (6U), injury (7G), or death (7H) may also be appropriate.

25-3. ARSON MOTIVES.

25-3.1. There are six (6) general motives for arson, as outlined in the "Crime Classification Manual," Douglas et. al, Lexington Books 1993; vandalism, excitement, revenge, crime concealment, profit, and extremist. Statistically, the first four listed are the most common motives seen in the military environment.

a. Vandalism. Vandalism-motivated arson is due to malicious and mischievous motivation that results in destruction or damage. The typical offender is a juvenile male. Educational facilities are a most common target. Other properties targeted are residential areas and vegetation.

b. Excitement. The excitement-motivated arsonist is prompted to set fires because he craves excitement that is satisfied by fire setting. The offender rarely intends the fire to harm people. The types of arsonists included in this category are thrill seekers, attention seekers, recognition, and sexual perversion. Common targets of the excitement-motivated arsonist are dumpsters, vegetation, lumber stacks, construction sites, and residential property. This fire setter may choose a site where he can watch fire suppression activity. The location of the fire will aid in identifying the motivation of the fire setter.

c. Revenge. A revenge-motivated fire is set in retaliation for some injustice, real or imagined, perceived by the offender. This offense may be a well-planned, one-time event, or the offender may be a serial arsonist taking revenge against society, with little or no pre-planning. Types of revenge-motivated arson include personal retaliation, societal retaliation, institutional retaliation, group retaliation, and intimidation. The targeted property often varies with the sex of the offender. The female arsonist will generally attack targets in or close to the home, whereas the male will tend to attack targets away from the home environment. In general, residential property and vehicles are prime targets. Arsonists who seek revenge against society may exhibit displaced aggression by choosing targets at random. Other offenders retaliate against institutions such as churches, government facilities, universities, or corporations.

d. Crime Concealment. This motive presents a more complex problem to the investigating agent; he may very well be investigating more than one crime, with a fire having been set to destroy evidence associated with the first crime(s). Such situations could involve homicides, burglaries, or the fire could have been targeted at destroying documents that reveal fraud. The targeted property is dependent on the nature of the concealment. The investigating agent must be alert to the presence of evidence of the other crime. For example, if a body is discovered in

the fire debris, the possibility of a homicide must be considered. The investigator must process this scene as two investigations; a fire investigation to determine origin and cause, and a homicide investigation.

e. Profit. Arson for profit is a fire set for the purpose of achieving material gain, either directly or indirectly. It is a commercial crime and exhibits the least passion of any of the motivations that generate the crime of arson. The types of profit-motivated arson found in this category are fraud to collect insurance, fraud to liquidate property, fraud to dissolve business, fraud to conceal loss or liquidate inventory, employment, parcel clearance, and competition. The property targeted by arson for profit includes residential property, business, and modes of transportation (vehicles, boats). This motive is rare, but not unknown, in the military environment, particularly considering its prevalence in the civilian community.

f. Extremists. Arson or bombings that are motivated by extremism can be the result of a psychological problem, an extreme political or social view, or both. Extremists will generally target groups, individuals, or locations because of personal aspects such as the race, religious affiliation, or ethnic origin of the target or as the result of their political differences. In some cases where a psychological disorder results in the extremist view, the targets may only be recognized by the offender and have no obvious or logical affiliations, as in the case of the Unabomber incidents.

g. An individual's motivation for starting a fire is never as clear-cut as these categories appear to be. There will be overlap in most cases, e.g., delay of deployment could be a motive, which may overlap between vandalism and revenge.

25-4. PROBLEMS IN ARSON INVESTIGATIONS.

25-4.1. Unique problems encountered in arson investigations include unusual difficulty in establishing intent. Arson investigations often require expert opinion testimony on the part of the investigator to establish that a crime has been committed.

25-4.2. In most types of investigation, the fact that a crime has been committed is readily apparent; however, at a fire scene, most of the evidence of the cause of the fire has been altered to such an extent that it may not easily be recognized as evidence. Often the only evidence that is obtained to take a suspect to court is circumstantial. Direct evidence of arson, such as an eyewitness, is rare. In the absence of direct evidence, circumstantial evidence must establish the cause as intentional, or, at least, eliminate all accidental or natural causes of the fire.

25-4.3. In cases where the cause of a fire is not readily apparent, an expert fire investigator is needed at the scene to recognize evidence, determine the location(s) or the origin(s) of the fire, and then to determine the cause. The expert fire investigator may subsequently be required in the courtroom to qualify as an expert witness to present evidence and to render opinion testimony.

25-4.4. Needed expertise must often be obtained from outside NCIS. The Navy employs Area Fire Marshals and Fire Protection Engineers who are charged with the responsibility of

investigating suspicious fires and fires causing damage amounting to over $50,000 that occur ashore, and such personnel may be requested to provide assistance to afloat units, depending upon their availability. This investigative responsibility is not intended to interfere with or replace NCIS investigative activities. Similar expertise may also be found within naval facility fire departments, and most states and municipalities within the United States maintain arson investigative agencies whose services may be called upon depending upon the local situation. Their expertise can be utilized at the fire scene, during subsequent investigation, and while preparing and presenting an investigation for court. Caution must be exercised when working with fire investigators. These persons may possess a high degree of expertise in fire investigation, but they may not be well acquainted with the legal aspects of the collection and preservation of evidence for laboratory analysis or trial in the federal court system. NCIS special agents must work very closely with such expert fire investigators in order to ensure that evidence is properly gathered and preserved. The role of the expert fire investigator in the investigation of arson fires is analogous to the role of the pathologist in homicide investigations; both make use of experienced opinion to establish cause.

25-5. STRUCTURE FIRES.

25-5.1. Procedures to be undertaken in the investigation of arson cases presented in the following paragraphs will not contain technical information concerning determination of the origin and cause of fires. This information and the techniques employed are far too extensive for presentation in this manual. It will suffice that the special agent realizes when expert assistance is required.

25-5.2. Response. In most cases, a determination has been made prior to the arrival of the special agent that the fire may be arson. Upon arrival at the fire scene, the special agent's first course of action should be to interview the senior fire official(s) present. It should be realized that the senior fire official has control over the fire scene until the fire is out and overhaul (clean up) is completed by fire suppression personnel. At a minimum, this interview should surface:

a. The rationale for arriving at the conclusion that the fire is arson,

b. The basic facts surrounding the fire from alarm to extinguishment,

c. The suspension of all overhaul duties, and

d. The Special Agent should obtain the cooperation and assistance of the senior fire official and his subordinates.

25-5.3. If investigation by NCIS is warranted, control of the fire scene should be assumed by the agent once the fire is completely extinguished. The scene must then be secured to exclude all others except NCIS special agents and personnel in their company. Standard fire department overhaul procedures should be postponed, and a command post should be established near, but not within, the fire scene.

25-5.4. A preliminary survey of the scene and the general area should then be conducted to

assess the situation, preserve perishable evidence, and identify witnesses before they lose interest and leave the scene. Agents may wish to consider photographing or video taping onlookers as arsonists often return to the scene to observe suppression and investigative efforts. Once the situation is assessed and perishable aspects have been preserved, expert assistance should be arranged for, if warranted, and additional Special Agents assigned to the investigation as required.

25-5.5. Data Collection. A considerable amount of valuable information will be available following a fire, and should be collected as the situation warrants.

a. With regard to fires ashore, maps of the general area involved should be collected, and with regard to fires either afloat or ashore, construction plans of the burned structure can be valuable and should be collected.

b. Shore installation fire departments are required to prepare a written fire report within twenty-four hours. This report should contain a narrative chronology of events surrounding the fire from alarm to extinguishment, including a summary of suppression efforts, and also includes a conclusion of the cause of the fire. Given this time constraint, it is obvious that a definite conclusion as to the cause of the fire in the fire report might be premature and consequently prejudicial to the administration of justice. Therefore, the special agent should be sensitive to this possibility and confer with the senior fire official accordingly. The conclusion of "under investigation" is the best for the fire department's report.

c. Weather conditions are sometimes of importance with regard to the progress of the fire, and that data should be collected. Weather facilities retain such information for considerable periods of time and the information can be collected when convenient.

d. The following persons should be identified for subsequent interview:

(1) The witness who sounded the original fire alarm is often one of the best sources concerning the earliest and therefore most important, stages of the fire. Usually the fire department will have this information on record, as well as the exact time and manner in which the alarm was received.

(2) Fire suppression personnel, particularly the first to arrive and enter the burning structure, can provide technical information which can be very helpful in determining the origin(s) of the fire. Fire suppression personnel will also be able to detail how the fire was fought.

(3) Security personnel associated with the structure burned, e.g., fire watches, masters-at-arms, roving patrols, sentries, etc.

(4) Occupants of the structure or the person(s) who is/are most familiar with the intimate details of the condition of the structure burned and its contents and occupants, immediately preceding the fire.

(5) Potential witnesses in the area, e.g., persons on duty in adjacent structures, known passers-by.

25-5.6. Interviews. Interviews of all those persons identified above should be conducted as applicable. If a witness has information concerning the early stages and/or progress of the fire, consideration should be given to participation of the fire investigation expert in the interview. Additionally, it is often useful to make use of the collected area maps and construction plans in complicated situations to locate witnesses, suspects, and points of interest. These interviews should cover the following general points:

a. The location(s) of the witness during the applicable time frame.

b. The location(s) of other persons observed by the witness during this time frame and their activities.

c. Background information on the structure, its contents, activities engaged in within the structure, and information concerning personnel associated with it.

d. Observations of the fire to include: colors of smoke and flames; amounts of smoke and flame; the intensity and progress of the fire; and any unusual sights, sounds, or odors associated with the fire.

25-5.7. Fire Scene Examination. Of equal importance to data collection and interviews is the fire scene examination that should commence as soon as possible. Consideration should be given to the need for and availability of an expert, adverse weather conditions which might destroy evidence, safety of the structure, the availability of enough light for a productive examination, and the priority of investigative leads and the available manpower to accomplish them. Agents should be in contact with their servicing Forensic Consultant (FC) and Major Case Response Team (MCRT) leader to arrange for a coordinated response to the scene.

a. The detailed examination of the scene of a large fire is a very painstaking procedure. It is lengthy, delves into minute detail, and is a very dirty business.

b. Very extensive note taking is usually required, and consideration should be given to the use of a portable tape recorder in order to ensure that all details are recorded. Minute details are especially important in fire investigations, for they may become of prime significance in reconstructing the scene after physical conditions have perished.

c. Extensive photography is necessary at scenes of major fires to ensure that all details are covered. Fire scenes present many unusual photographic situations on a routine basis. Automatic settings on even the most expensive cameras usually result in poor photographs. The services of the servicing FC or highly competent photographer from the MCRT or command should be utilized in complicated situations.

d. Making use of existing floor/construction plans will save time in preparing a rough scene sketch, locating evidence, points of interest, and photograph positions. These plans can

also be of use in locating and tracing the structures' electrical, gas, and ventilation systems, as well as provide information indicating if these systems have been altered to present a fire hazard.

e. In conducting a fire scene examination with the aid of an expert, the MCRT should assist the expert in his efforts to determine the origin and cause of the fire, and collect and preserve evidence of the origin and cause through note taking, sketching, and photography. It would be inadvisable under most circumstances to depend upon the expert to collect and preserve this evidence. The MCRT should consider the team to be solely responsible for the collection and preservation of evidence of other crimes and collection of evidence with which to identify the perpetrator.

25-5.8. Detailed Fire Scene Examination Procedures. The following procedures are applicable to a large fire in a structure, and are therefore not pertinent to all types of fire scenes. However, their utilization should be readily apparent in different situations:

(b)(7)(E)

25-5.9. Follow-up investigation may include, but is not limited to, interviews of Sources (levels

(b)(7)(E)

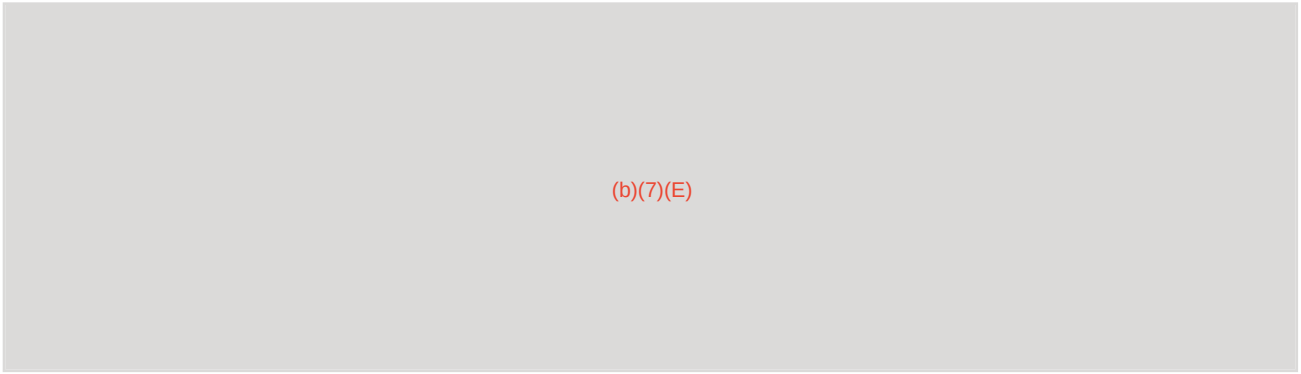
25-6. VEHICLE FIRES.

25-6.1. NCIS investigation of vehicle fires or fires involving mobile homes can result from several situations: An individual may report his/her vehicle stolen and it is subsequently recovered as a burned-out hulk; an individual may report someone set his/her car afire; or that the car became engulfed in flames as a result of alleged mechanical failure. In any case, the investigation must be able to substantiate the fire was arson. Determining who was responsible for setting the fire is obviously an investigative goal and uncovering the motive for setting the fire, especially in the case of owner complicity, often requires considerable investigative effort. Article 134, UCMJ, includes "burning with intent to defraud" which carries a maximum punishment of ten years confinement and a dishonorable discharge. It should be noted that the accused does not actually have to submit a claim to the U.S. Government or to an insurance company for the offense to be consummated. (See also NCIS-3, Section 27 regarding vehicle thefts.)

25-6.2. Response. Upon receiving a complaint that suspicious circumstances surround a vehicle fire, secure the vehicle and the surrounding area. The area around the vehicle should be examined for cans, bottles, or other containers that may have held a liquid accelerant. Depending on the terrain, the search area could be quite large. Check the scene for footwear impressions and tire tracks. Soil samples to a depth of several inches from under or around the vehicle may yield traces of a flammable/combustible liquid. A complete set of photographs of the scene should be taken; interior and exterior. In some cases latent fingerprints can be developed from interior and exterior surfaces for future comparison but may require specialized or crime laboratory techniques.

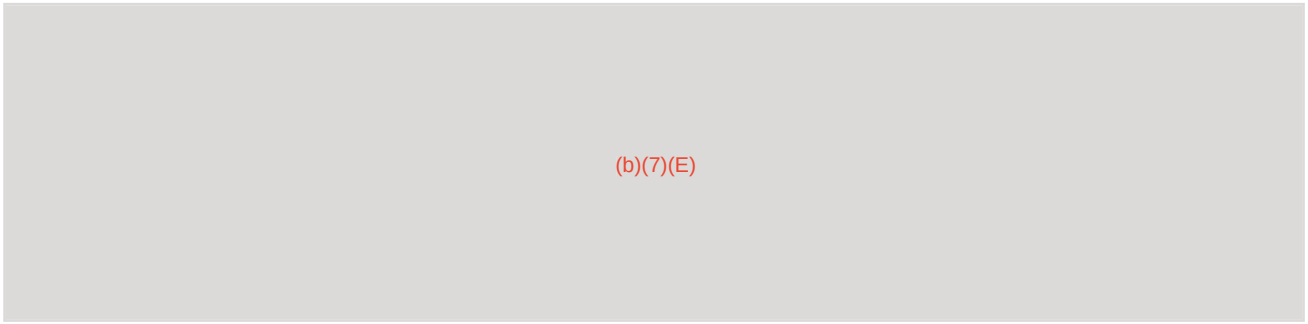
(b)(7)(E)

Page 743 redacted for the following reason:
- - - - - - - - - - - - - - - - - - - -
(b)(7)(E)



25-7. FLAMMABLE LIQUIDS.

25-7.1. Because of their prevalent use as accelerants, flammable/combustible liquids are given some attention in the following paragraphs. Volatile liquids represent evidence that is particularly difficult to locate, collect, and preserve. However, if found and properly handled, such evidence often may provide proof of the willful and malicious element of the offense of arson.



b. Many fire departments utilize apparatus known as flammable vapor detection devices which will not only identify vapors as flammable, but will measure their concentration in parts per million.

c. In the same vein, ATF and some fire investigation agencies employ the use of dogs trained in the detection of accelerants. The use of such an asset cannot be underestimated in the conduct of a fire investigation.

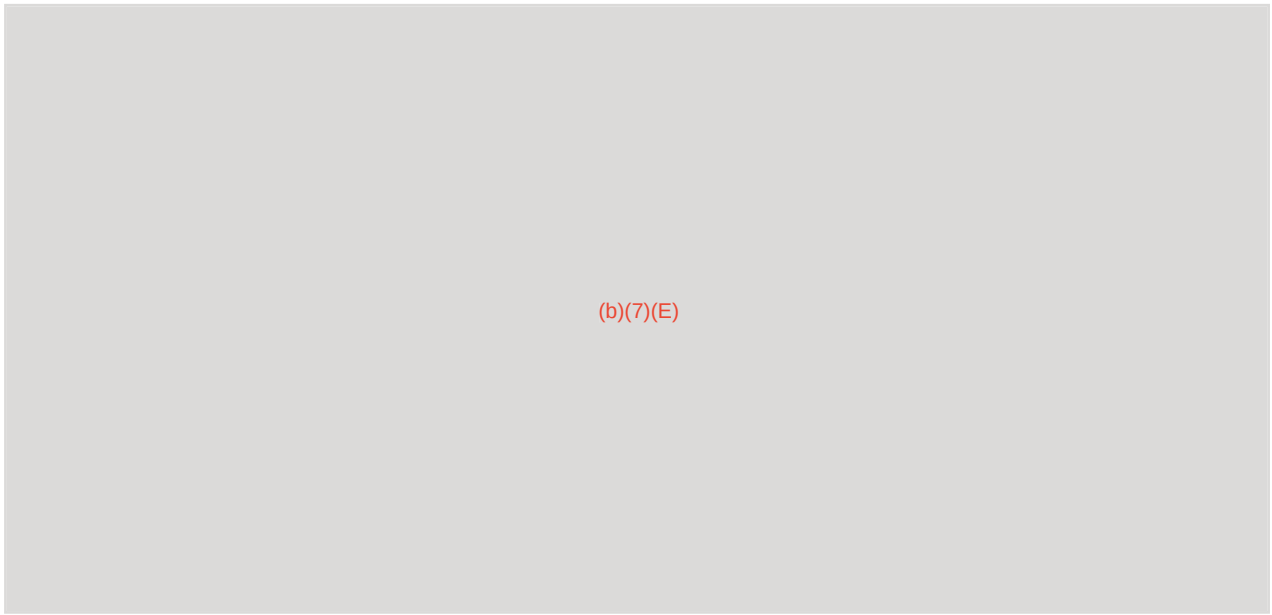
d. Regarding run-off water resultant from fire fighting, it can be generally stated that if a film of suspected liquid accelerant cannot be observed floating on top of the water, it is not worth collecting. The best rule to follow with regard to suspected liquid accelerant is if you can see it or smell it, collect it.

e. The experienced fire investigator is aware of many indicators in fire patterns that tell him/her that a liquid accelerant has probably been used. It is good practice to depend upon the fire investigator to locate suspicious areas for the collection of debris samples.

f. When collecting samples suspected of containing liquid accelerant residue, the best containers are new, unlined, metal paint cans. The container must be air-tight, as the liquid

vaporizes. Plastic containers, particularly plastic bags, will often test positive for the presence of accelerants and are not useful for this type of evidence. As soon as suspected debris is detected, it should immediately be placed in a suitable container, sealed, labeled, photographed, and seized. If any container other than a clean metal can is used, to include glass containers, nylon bags or bottles, a clean, unused example of the container used will be forwarded to the laboratory with the seized evidence as a control for the examiner. The servicing laboratory will dictate the specified manner by which evidence is packaged. Thus it is important to make contact with the servicing laboratory early in the investigative process.

25-7.2. Preservation of flammable/combustible liquids is a most difficult problem, and time is the worst enemy. By their nature, flammable/combustible liquids are constantly evaporating into the air and their rate of vaporization increases with a rise in temperature. A good starting point for determining the rate of vaporization of a particular liquid is its flashpoint, or the temperature at which an ignition source will produce a flash, but not a self sustained combustion at the surface of the liquid. However, the vaporization rate will always be directly proportional to the ambient temperature. For example:



25-8. BOMB INCIDENT AND POST BLAST INVESTIGATIONS.

25-8.1. The investigation of a bomb incident and a post-blast scene present special problems for the agent, specifically in regards to safety. First and foremost, the special agent responding to the scene of a recovered explosive device or an actual explosion must remember that secondary devices and/or unexploded portions of the initial device may be present at the scene. Therefore, NO BOMB/BLAST SCENE INVESTIGATION SHOULD EVER BE CONDUCTED UNTIL THE AREA OF THE BLAST AND THE SURROUNDING VENUES HAVE BEEN THOROUGHLY SEARCHED FOR ADDITIONAL DEVICES. SPECIAL AGENTS OF THE NCIS ARE NOT TRAINED AS BOMB TECHNICIANS AND WILL NOT ATTEMPT TO DISARM EXPLOSIVE DEVICES.

25-8.2. Once an area has been determined to be free of unexploded materials and secondary devices, the area should be cleared of all unnecessary personnel and a preliminary examination of the area should be conducted.

25-8.3. Recovered Device.

a. Many explosive devices fail to function for a variety of reasons. They may have been intentionally designed not to detonate, they may have failed as the result of improper design or fabrication, or they may have been disarmed by a trained Explosive Ordinance Disposal (EOD) technician or a "lucky amateur." In these cases, the technician may feel that the device is safe to seize as evidence or may elect to either transport it to a safe location or evacuate an appropriate area and conduct a controlled detonation of the device. Should the technician elect to destroy the device through a controlled detonation, the special agent will in no way attempt to dissuade the technician from the chosen course of action. The agent may certainly request that if a less destructive method is available to the technician that it be employed if possible, always of course leaving the decision to the EOD technician. If permissible and safe, the special agent should request the technician to photograph the device prior to moving it or destroying it.

b. If the device is rendered safe by destruction, the blast should be video taped if at all possible. The resulting debris from the device will be collected for examination and analysis. Additionally, the EOD technician will be interviewed in depth for information concerning the manner in which the device was assembled, his/her opinion of the level of knowledge or expertise held by the builder of the device, and the nature of the materials and explosives used to assemble the device.

c. In circumstances where the device has been rendered safe by the EOD technician without destruction, the device will be photographed in place and the EOD technician will be interviewed to determine what changes he/she made to the device in order to disarm it (wires cut, batteries removed, etc). The device, once removed from the scene by the technician, should be examined by either the FBI or ATF bomb centers. The explosive and detonators recovered from the device should be stored at an EOD facility for safety.

d. In all cases involving unexploded devices, the use of any transmitting equipment, including police radios, cellular telephones, CB radios, or any related equipment which require the use of transmitting frequencies will not be used.

25-8.4. Post-Blast Crime Scene.

a. Immediately following a detonation, confusion will be the order of the day. While there is little or nothing that the responding agent can do to eliminate the confusion at the scene, every effort should be made, in conjunction with available security and command personnel, to cordon off and preserve the immediate blast scene, allow for the prompt evacuation of casualties, and insure that all appropriate agencies and commands are notified of the incident. Once this has been accomplished, the blast scene examination can begin.

b. Preliminary Phase. The preliminary examination will endeavor to find the farthest

extent of the blast debris. During this phase, no evidence will be documented or seized but the full extent of the scene will be established and the perimeter set. The standard formula for establishing a blast scene perimeter is to extend an imaginary line from the center of the blast to the farthest piece of debris found and construct an imaginary circle, this will establish the inner perimeter. After the inner perimeter has been established, a distance no less than half of the radius of the inner circle will be used to establish a second circle which will serve as the outer perimeter. The command post, liaison sites, and evidence examination will be conducted outside the outer perimeter.

c. Additionally, during the preliminary examination, blast damage, primarily broken glass but generally any damage done by the shock wave of the blast, will be identified and the farthest identifiable blast damage and the distance and direction from the blast center will be identified and noted.

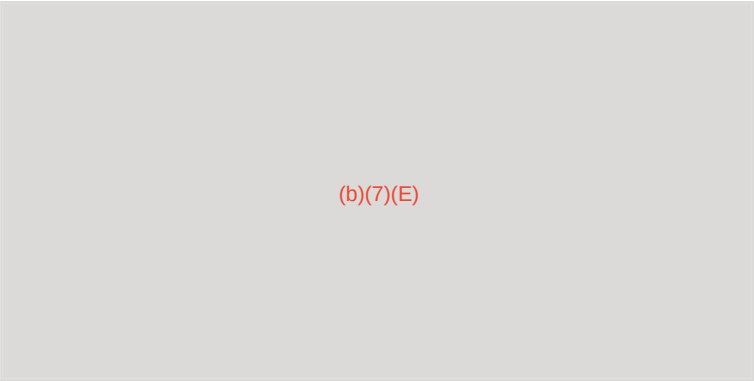
d. In circumstances where a blast has occurred in or adjacent to a building or structure and that building or structure has suffered structural damage, no special agent or investigative personnel should enter that structure for the purpose of investigation until the structure has been examined and safe/unsafe areas clearly designated.

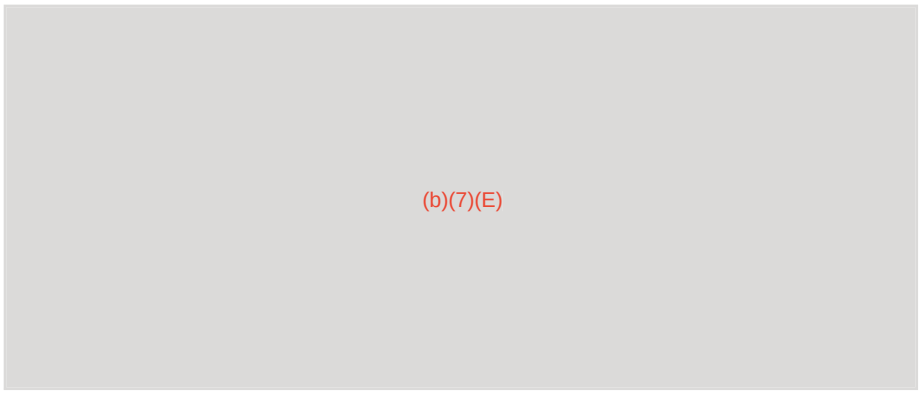
e. Weather and weather patterns that existed at the time of the explosion should be noted, along with any unusual circumstances.

f. Once a blast scene perimeter is established, the area can be examined for debris and items of evidence. As in all crime scene examinations, no item will be moved until documented, sketched, and photographed. Should blast damage or debris be found outside the inner perimeter of the scene, the inner and outer perimeters should be re-established at the outer-most point.

25-8.5. Primary Examination. The primary examination will generally be conducted by a trained post-blast investigator. NCIS Forensic Consultants (FC) and a number of MCRT members have received Basic Post-Blast training and most FCs have been trained in Advanced Post-Blast Investigations.

25-8.6. Witness Interview. Interviews of individuals at or near the scene of a blast incident should be conducted as soon as possible. Videotape and still photography taken at the scene should be obtained for examination and duplication. Questions asked of these individuals should include, but should not be limited to:





25-8.7. General Investigation.

a. The blast scene investigation will be conducted under the direction of the post blast investigator.

b. Evidence seized will be sorted and transported to the crime lab or Bomb Center for detailed examination. While an experienced post blast investigator may be able to hypothesize on the nature, type, and amount of explosive used and the type of device used in its delivery, it is the responsibility of the examining laboratory and bomb center to make these determinations. The working hypothesis in such investigations will not be discussed with any group or individual not involved in the actual investigation. The premature release of information be it accurate or inaccurate, can have a detrimental effect on the conduct of the investigation.

c. Investigation conducted at the scene and in the field, based on either the laboratory report or the working hypothesis of the post blast investigator, will center on the identification of the individual(s) who fabricated the device and the motive for its use. The best method for trying to establish this is an analysis of the target. Target analysis, in bombing cases, will generally identify the motive of the individual(s) responsible. When coupled with certain knowledge of the materials used and the method of delivery, as provided by the laboratory, the bombers motives, access to materials, and relative expertise will be identifiable and standard investigative techniques will serve for the conduct of the balance of the investigation.

25-8.8. Motivation. As in arson investigations, vandalism, excitement, revenge, extremism and crime concealment, or any combination thereof, can be primary motives for fabrication and/or detonation of an explosive device. However, in the use of explosives the agent must also note that the use of an explosive device as the primary instrument for the commission of a homicide, robbery, or other criminal offense (extortion, assault, arson, etc.) is common. Likewise, explosives are often the weapon of choice in acts of political terrorism (domestic, foreign, state-sponsored, etc.) or for the psychologically maladjusted. Regardless of motive, a psychological profile of the bomber can be an invaluable tool in the conduct of such inquiries. Assistance in developing a psychological profile can be obtained by contacting the NCISHQ program manager for Bomb and Arson investigations.

25-9. APPLICABLE LAWS.

a. UCMJ Article 126.

(1) Any person subject to this chapter who willfully and maliciously burns or sets on fire an inhabited dwelling, or any other structure, movable or immovable, wherein to the knowledge of the offender there is at the time a human being, is guilty of aggravated arson and shall be punished as a court-martial may direct.

(2) Any person subject to this chapter who willfully and maliciously burns or sets fire to the property of another, except as provided in subsection (a), is guilty of simple arson and shall be punished as a court-martial may direct.

b. UCMJ Article 134. This article includes "burning with intent to defraud," which carries a maximum punishment of ten years confinement at hard labor and a dishonorable discharge.

c. Title 18 USC 81. Arson within special maritime and territorial jurisdiction.

d. Title 18 USC 841-48 are the explosives violations.

(1) Title 18 USC 844(I) applies to explosives and therefore may allow federal authorities such as ATF to enter a case when, under certain circumstances, gasoline was used. Legislation introduced during 1982, and signed by President Reagan in October of that year, modified this section to include the word "fire" in addition to "explosion."

e. Title 18 USC 1855. Wildlands Fires.

f. Title 26 USC 5861. Destructive Devices.

g. Organized Crime Control Act Of 1970 (18 USC 842 AND 844 (D))

CHAPTER 26
TITLE: BURGLARY (CATEGORY 6N)
POC: CODE 23A
DATE: SEP 07

26-1. DISCUSSION.

26-1.1. General. Burglary and its related offenses, Housebreaking and Unlawful Entry, are property related crimes that may also constitute personal crimes depending on the circumstances and intent of the suspect.

26-1.2. Definitions.

a. Burglary: Breaking and entering in the nighttime of a dwelling house with the intent to commit a felony.

b. Housebreaking: Unlawfully entering a structure or building with the intent to commit any crime.

c. Unlawful Entry: Illegally entering a dwelling, building or structure.

d. Dwelling House: A location or construct that is occupied as a residence, such as any private rooms, apartments, mobile homes, trailers and similar vehicles and includes outbuildings within a common enclosure, such as a tool shed inside the fence of a backyard.

e. Breaking: Creating a breach or opening, such as opening a door or window sufficiently to gain entry. There may also be a constructive breaking, such as gaining entry by trick, such as concealing oneself in a box.

f. Entering: The physical action, no matter how slight, of affecting entry into the location.

g. Building: A location or edifice, such as a room, shop, store, office, or apartment building; not necessarily occupied.

h: Structure: Refers to spaces, locations or constructs that are in the nature of a building or dwelling, such as a stateroom, hold, inhabitable trailer, tent, freight car, or houseboat.

26-1.3. Criminal Law/Jurisdiction.

a. Uniform Code of Military Justice. Crimes of this category are potentially violations of UCMJ:

Article 129 (Burglary)
Article 130 (Housebreaking)
Article 134 (General Article - Unlawful Entry)

Along with consideration for attempts and conspiracies.

b. Federal Law/United States Code (USC). Crimes of this category are potentially violations of Title 18 USC Chapter 103 - Robbery and Burglary.

Section 2111 (Special Maritime and Territorial Jurisdiction)
Section 2112 (Personal Property of the U.S.)
Section 2113 (Bank Robbery and Incidental Crimes)
Section 2115 (Post Offices)
Section 2117 (Breaking or Entering Carrier Facilities)
Section 2118 (Robberies and Burglaries Involving Controlled Substances)

Along with consideration for attempts and conspiracies. Crimes in this category that occur in federal jurisdiction, which are not directly covered under federal law but are violations under local or state law, may be potentially investigated through the Assimilative Crimes Act, Title 18 USC Section 13.

c. State Criminal Law. Depending on jurisdiction and/or victim of crimes of this category (i.e., government property), appropriate state penal code may apply. Under some state's criminal code, Unlawful Entry may be the same as Trespass.

26-2. POLICY AND GUIDANCE.

26-2.1. NCIS Authority. NCIS authority and jurisdiction to investigate this category of offenses is derived from SECNAVINST 5430.107. DOD Directive 5525.7 implements the Memorandum of Understanding (MOU) between the Department of Justice and the DOD criminal investigative organizations. This MOU provides policy and guidance for criminal investigations when both departments have jurisdiction. See NCIS-3, Chapter 1 (Authority, Jurisdiction, Scope) for further explanation.

26-2.2. NCIS Responsibility.

a. NCIS can investigate any suspected Burglary or Housebreaking to determine if it constitutes either of those crimes. NCIS will not normally investigate the offense of Unlawful Entry as a crime unto itself; however, it may be utilized as a lesser-included offense in an investigation.

b. The case category 6N (Burglary) should be retained unless the other offense is more serious, such as murder, manslaughter, or rape; in which case, the category for the more serious offense should be assigned.

c. If NCIS responds to a complaint of Burglary or Housebreaking, a detailed crime scene examination should occur, to include photographs, diagrams/sketches, evidence collection and taking any victim and/or witness statements. Attempts should be made to employ forensic techniques as appropriate, such as latent fingerprint or tool mark examination.

d. If an NCIS investigation is opened on a Burglary or Housebreaking, liaison with the local security force and/or police departments of adjacent communities should occur. Any police reports or incident reports made by other law enforcement entities should be requested as part of the investigation.

e. The investigating agent should take written statements from the victim and pertinent witnesses, such as the individual who discovered the break-in. Statements should be taken of interrogated suspects.

26-3. ELEMENTS OF THE CRIME.

26-3.1. Essential Elements. Within the Burglary-type crimes and the related Housebreaking and Unlawful Entry offenses under the UCMJ, the essential elements will involve breaking and/or entering into a dwelling, building, or structure. Under Federal and State laws, the definitions and elements of Burglary may be different than in the UCMJ. Housebreaking may not exist under State law, but its elements may be under the State legal interpretation of Burglary. Furthermore, under state law Unlawful Entry maybe the same as Trespass.

26-3.2. Elements of Burglary. The elements of Burglary under the UCMJ are:

a. That the accused unlawfully broke and entered the dwelling house of another,

b. That both the breaking and entering were done in the nighttime, and

c. That the breaking and entering were done with the intent to commit an offense punishable under UCMJ Articles 118 through 128 (with exception of Article 123a).

(1) Articles 118 through 128 are the offenses of murder, manslaughter, rape and carnal knowledge, larceny and wrongful appropriation, robbery, forgery, maiming, sodomy, arson, extortion, and assault.

26-3.3. Legal Discussion – Burglary.

a. It is immaterial whether the offense intended is committed or even attempted. If the offense is actually intended, at the time of entry, it is no defense that its commission was impossible.

b. To constitute Burglary, the house must be the dwelling house of another. The structure must be used as a dwelling at the time of the breaking and entering, although it is not necessary that anyone actually be in the structure at the time of the offense. If the structure has never been occupied at all (such as a newly constructed house) or it has been left with no intention of occupying it again (e.g., a vacated house), it is not a dwelling house. A tent is not a subject of burglary.

c. There must be a breaking, either actual or constructive. Merely to enter through an existing opening such as an open window or door or hole does not constitute a breaking. If there is a removal of any part of the dwelling designed to prevent entry there is a breaking. Opening a closed door or window or opening wider a window or door that would have been insufficient to enter through is considered a breaking. The breaking of an inner door by one who is lawfully inside a dwelling, but who has no authority to enter the inner room, constitutes a burglary as long as the requisite intent is present and entry is made.

d. 'Actual' breaking is made when entry is gained through physical force or movement.

e. Constructive breaking is made when the entry is gained by a trick, under false pretense, by intimidation, or through collusion with a confederate.

f. Entry must be affected before the offense is completed, but the entry of any part of the body, even a finger, is sufficient, and an insertion into the house of an instrument or tool, except merely to facilitate further entrance, is a sufficient entry.

g. Both the breaking and entering must occur in the nighttime, which is the period between sunset and sunrise when there is not sufficient daylight to discern a person's face, and both must be done with the intent to commit in the dwelling an offense punishable under the Articles 118 through 128 (except Article 123a) of the UCMJ.

26-3.4. Elements of Housebreaking. The elements of Housebreaking under the UCMJ are as follows:

a. That the accused unlawfully entered a certain building or structure of another person, and

b. That the unlawful entry was made with the intent to commit a criminal offense therein.

26-3.5 Legal Discussion – Housebreaking.

a. The offense of Housebreaking is much more broad than that of Burglary in that the place that is entered is not required to be a dwelling house, meaning it is not necessarily a place that is occupied. It is not essential that that there is a breaking and the entry can occur during the nighttime or daytime. The intent to enter need not be to commit one of the specific offenses listed under Burglary. It is not necessary for the building or structure to be in use at the time of entry.

b. Proof of the intent to commit *some kind of* criminal offense is essential to support a conviction for Housebreaking. Any act or omission punishable by court-martial, except one constituting a purely military offense, is a 'criminal offense.'

26-3.6. Unlawful Entry. This offense involves the mere unlawful entry of any building or structure as defined for the offense of Housebreaking, without any additional elements. The intent of the offender is irrelevant and need not be established. Unlawful Entry is a lesser-included offense (Article 134 – General Article) of Burglary and/or Housebreaking.

26-4. INVESTIGATIVE PROCEDURE.

26-4.1. Considerations.

a. Since both Burglary and Housebreaking involve the intent to commit another offense, in many cases that other offense(s), i.e., larceny, rape, will also have been committed or attempted. The investigation should therefore be directed to the acquisition of evidence relating to both offenses; the burglary or housebreaking and the other offense(s).

b. Common targets for burglary and housebreaking include military exchange facilities for money and consumer goods; offices for office equipment, blank military identification cards, payroll checks, personnel records, and advancement tests; club facilities for money and consumer goods; warehouses for stored merchandise and military equipment; armories for ordnance and weapons; disbursing offices for money and checks; post offices for money, stamps, and money order blanks; medical facilities for drugs; and housing for money, personal goods, and sexual assault.

c. Common methods of entry include use of key or lock combination obtained by subterfuge or from confederates; hiding in the building until it is secured; forcing padlocks with bolt cutters, prying device, hammering tool, or hacksaw; insertion of thin instruments to release spring locks; cutting window screens and breaking windows; leaving doors or windows unlocked and returning after working hours; and penetrating roofs through ventilation systems or by cutting holes.

d. Security containers (safes) are most commonly entered by peeling away doorplates, punching out dials, drilling out the locking mechanism, or carrying them away from the premises. They are less commonly forced open by attacking them with welding equipment or explosives. Some very common practices by safe custodians

which aid the thief are failing to lock the combination lock of a security container, and securing it only with a padlock; dialing in all but the last number of the combination to facilitate opening the safe on the following day; setting combinations using birthdates or other numbers the thief could surmise; carelessly operating the combination in view of potential thieves; failing to change the combination when a new custodian assumes control of the safe; and secreting the written combination nearby the safe, where a thief could find it.

e. Common suspects include past and present military and civilian employees of the target facility; janitorial personnel; dependent minors; sentries assigned to protect the target facility; and in overseas areas, natives in the local area. Personnel suspected of having financial difficulties, narcotics habits, or who habitually overindulge in vices, are particularly suspect, as well as military or civilian personnel who were recently or are about to be separated or transferred from the target facility.

f. The investigating agent should make logical attempts to locate stolen goods disposed of by the suspect through NCIC, pawnshop coverage, online searches (such as through Ebay or Yahoo Auctions), lawful search and seizure, interrogations and the development and utilization of cooperating witnesses. All of these steps should be directed at firmly establishing, through evidence presentable in the courtroom, the elements of the offense under investigation and the identity of the culpable party.

g. Some countermeasures which the special agent can recommend to victimized commands include security patrols, alarm systems, security education of personnel, improved locking devices and building security features, better containers for valuables, improved lighting, and the recording of serial numbers of high value items for later identification. High value items that have no serial numbers and highly pilferable items should be marked in some unique fashion for later identification.

26-4.2. Procedure.

a. When conducting investigations of burglary offenses, NCIS special agents should be alert to the very specific nature of the elements of this offense, as set forth, supra, and gather sufficient evidence to support each element. Any or all investigative procedures and resources in this manual, coupled with the special agent's own initiative, imagination, and resourcefulness may be applicable in any investigation.

b. Photographs of evidence of the breaking are important; latent evidence of entry in the absence of witnesses is necessary; the time of day must be documented; and the status of the structure as a dwelling must be established. In the absence of the actual commission of one of the delineated offenses requisite for burglary, particular care must be taken to establish the intent at the time of the breaking and entry. Should the suspect make admissions and provide a written statement, his intentions should be carefully and clearly documented.

c. The crime scene examination is a very important aspect of these types of investigations. Initially, the special agent should insure that the crime scene is secured and protected from other persons and the elements. Following interviews of initial witnesses, or concurrently if manpower is available, the crime scene should be examined in a systematic and painstaking manner. In examining the crime scene, the special agent should keep in mind that he is looking for two types of physical evidence: evidence of the crime itself (corpus delicti), and evidence that might lead to the identity of the culpable party (trace evidence). The objective of the crime scene examination is to locate this evidence; identify, photograph, and/or include it in the crime scene sketch; and collect and preserve it.

(1) Evidence of the corpus delicti can include the point and method of entry, the object of the entry, the point and method of exit, the time of entry, and objects of value taken and not taken by the suspect.

(b)(7)(E)

CHAPTER 27
TITLE: LARCENY
POC: CODE 23A
DATE: FEB 08

27-1. DISCUSSION

27-1.1. General. Larceny and its related offenses are property crimes involving the unlawful taking of property, the transfer of stolen property and/or the receipt of stolen property. The following subcategories are used in larceny investigations:

a. (6S) Larceny - Government,

b. (6R) Larceny - Ordnance,

c. (6T) Larceny - Personal,

d. (6V) Larceny - Vehicle, and

e. (6X) Special Inquiry (see NCIS-3 Chapter 28).

27-1.2. Definitions

a. Larceny. The unlawful taking or withholding of property from its owner with the intent to permanently deprive the owner of the property.

b. Wrongful Appropriation. The unlawful taking or withholding of property from its owner with the intent to temporarily deprive the owner of the property.

c. Embezzlement. The unlawful use or appropriation of an owner's property or money entrusted to the care of the accused.

d. Property. Anything of value possessed by the owner or other person authorized by the owner.

e. Possession. The act of care, custody, management, or control over the property.

27-1.3. Criminal Law/Jurisdiction

a. Uniform Code of Military Justice (UCMJ). Crimes of this category are potentially violations of UCMJ:

Article 121 (Larceny and Wrongful Appropriation)
Article 134 (General Article – Stolen Property: Knowingly Receiving, Buying or Concealing)
Article 134 (General Article – Obtaining Services Under False Pretenses)
Article 134 (General Article – Military Property of the US: Sale, Loss, Damage Destruction, or Wrongful Disposition)

Any possible violations should be considered for attempts and conspiracies. Larcenies involving the postal system, such as mail theft or destruction, are discussed in NCIS-3, Chapter 28 (Crimes Against Property – Other), under the Postal category (6L).

b. Federal Law/United States Code (USC). Crimes of this category are potentially violations of the following:

Title 18 USC Chapter 31 – Embezzlement and Theft,
Title 18 USC Chapter 44 – Firearms,
Title 18 USC Chapter 103 – Robbery and Burglary,
Title 18 USC Chapter 113 – Stolen Property,

Any possible violations should be considered for attempts and conspiracies. Crimes in this category that occur in federal jurisdiction, which are not directly covered under federal law but are violations under local or state law, may be potentially investigated through the Assimilative Crimes Act, Title 18 USC Section 13.

c. State Criminal Law. Depending on jurisdiction and/or victim of crimes of this category (e.g., government property), appropriate state penal code may apply.

27-2. POLICY AND GUIDANCE

27-2.1. Naval Criminal Investigative Service (NCIS) Authority. NCIS authority and jurisdiction to investigate this category of offenses is derived from SECNAVINST 5430.107. Department of Defense (DoD) Instruction 5525.07 implements the Memorandum of Understanding (MOU) between the Department of Justice and the DoD criminal investigative organizations. This MOU provides policy and guidance for criminal investigations when both departments have jurisdiction. See NCIS-3, Chapter 1 (Authority, Jurisdiction, Scope) for further explanation.

27-2.2. NCIS Responsibility

a. A major offense (felony level) for larceny (Article 121) under the UCMJ is that the alleged stolen government or personal property must have a value of more than $500.00. Therefore, in

relation to the UCMJ, NCIS has investigative jurisdiction in all thefts of U.S. Government or personal property/funds over $500.00.

b. Under U.S. Federal criminal code, generally, stolen property or monies valued at $1,000.00 or more are felony level crimes. Therefore, in relation to Federal law, NCIS can have investigative jurisdiction in thefts of U.S. Government or personal property/funds over $1,000.00.

c. However, for the purposes of standardization and the best utilization of NCIS investigative resources, NCISHQ has established a “dollar” threshold as a baseline for determining NCIS involvement in a larceny investigation. The following is an explanation of those thresholds:

(1) For government owned property, the threshold is set at $5,000.00. This is based on SECNAVINST 7320.10A (01APR04) ‘Department of the Navy (DON) Personal Property Policies and Procedures.’ In this instruction, the DON is required to account for property having an acquisition value of $5,000.00 or more (with exceptions for sensitive, pilferable, classified, critical, and hard to replace items).

(2) For personally owned property, the threshold is set at $2,500.00. This amount is viewed a quality of life issue for military personnel, since the loss of property of this value or greater is a significant loss, especially to junior enlisted personnel.

(3) The cognizant NCIS office, at their discretion, may initiate investigations below the thresholds when deemed appropriate due to circumstances, such as a series of unresolved minor losses within a command, or incidents deemed to have a substantial impact on a command’s morale and good order. Conversely, the cognizant NCIS office may decline investigations which exceed the threshold if, in the judgment of the supervisor, there are extenuating circumstances. The commencement of a NCIS larceny investigation below thresholds or of declining an investigation above the thresholds should be the exception, as NCIS seeks to achieve across the board standardization.

d. Requests for NCIS investigation based on routine inventory losses, with no evidence of theft, and complaints, that are too old for the completion of meaningful leads, should be declined.

e. Regardless of value, other larcenies that have legitimate or "special interest" to the DON should be investigated by NCIS (as per SECNAVINST 5430.107). Although not an all-inclusive list, NCIS specifically exempts the following from the “value” criteria:

(1) Theft of narcotics and controlled substances;

(2) Thefts of government firearms, ammunition, and explosives;

(3) Toxicological material;

(4) U.S. Treasury Checks (blank) and postal money orders; and

(5) Nuclear devices, components, etc.

f. The cognizant NCIS supervisor may exempt other larcenies of extraordinary or special interest to the DON. For example, the occasional loss of one or two military identification cards or the theft of a few rounds of small arms ammunition will also be left to the discretion of the NCIS supervisor, depending on all the facts and circumstances. The theft of military ID cards may not be a felony in itself, but the fraudulent use or sale (Article 134) of the cards can be punished by three years imprisonment or confinement. Thus, where evidence suggests possible fraudulent use, possession, or sale, an investigation may be warranted.

g. If NCIS investigates a complaint of a larceny, a detailed crime scene examination should occur, to include photographs, diagrams/sketches, evidence collection, and taking any victim and/or witness statements. Attempts should be made to employ forensic techniques as appropriate.

h. If a NCIS investigation is opened on a larceny, liaison with the local security force and/or police departments of adjacent communities should occur. Any police reports or incident reports made by other law enforcement entities should be requested as part of the investigation.

i. The investigating agent should take written statements from the victim, pertinent witnesses and from the interrogation of suspects.

j. Whenever several criminal offenses are referred to NCIS, the more serious crime (based on the Manual for Courts-Martial (MCM) Table of Maximum Punishments) will generally be the determining factor in the selection of the crime to be investigated. For instance, the elements of burglary or housebreaking are often present in larceny and, therefore, the more serious crime of burglary would likely be investigated. This does not preclude larceny from being handled as a lesser included offense.

k. Larcenies involving the mail/postal system should be investigated under the case category Postal (6L). The sale of stolen property can be reviewed for possible black marketeering, which is investigated under the case category Black Market (6C). See NCIS-3, Chapter 28 (Crimes Against Property – Other) for further explanation.

27-3. ELEMENTS OF THE CRIME

27-3.1. Essential Elements. A wrongful taking with intent to permanently deprive includes the common law offense of larceny. The wrongful obtaining with the intent to permanently defraud a person is the offense formerly known as “obtaining by false pretense.” The wrongful withholding with the intent permanently to appropriate is the offense formerly known as embezzlement. Both “obtaining by false pretense” and embezzlement may be charged and proved under a specification alleging that the accused “did steal” the property in question and therefore a potential violation of Article 121 (Larceny and Wrongful Appropriation) or Article 134 (General Article).

a. The subcategory 6S Larceny - Government is used for investigations pertaining to theft of property (except ordnance) owned in whole or in part by the government. Also included is the illegal possession or illegal sale of such government property, and thefts of property (except ordnance) from nonappropriated fund activities.

b. The subcategory 6T Larceny - Personal is used for investigations pertaining to the theft of property, other than government property, where there has been no force or violence employed. Included are theft of personal property, private property to include that property belonging to exchange concessionaires, and monies and properties of exempted nonappropriated fund activities.

27-3.2. Elements of Larceny. The elements of Larceny under the UCMJ are:

a. That the accused wrongfully took, obtained, or withheld certain property from the possession of the owner or of any other person;

b. That the property belonged to a certain person;

c. That the property was of a certain value, or of some value; and

d. That the taking, obtaining, or withholding by the accused was with the intent permanently to deprive or defraud another person of the use and benefit of the property or permanently to appropriate the property for the use of the accused or for any person other than the owner.

If the property is alleged to be military property (as defined in paragraph 32c(1) of the MCM) add the following element;

e. That the property was military property.

27-3.3. Legal Discussion – Larceny

a. There must be a taking, obtaining, or withholding of the property by the accused. Property cannot be "obtained" by merely acquiring the title of the property, without exercising some possession or control over the property. As a general rule, any movement of the property or any exercise of dominion over it is sufficient if accompanied by the requisite intent. For example, as long as the other elements of larceny are proved, enticing a person to transfer funds into the accused bank account or obtaining the delivery of another's goods to a person designated by the accused would be larceny.

b. A "withholding" may arise as a result of a failure to return, account for, or delivery is due, even if the owner has made no demand for the property. A "withholding" may also occur as a result of devoting property to a use not authorized by its owner.

c. Acts, which constitute the offense of unlawfully receiving, buying or concealing stolen property or of being an accessory after the fact, are not included within the meaning of "withholding." Therefore, neither a receiver of stolen property nor an accessory after the fact

can be convicted of larceny on that basis alone. The taking, obtaining, or withholding must be of specific property.

d. The "owner" refers to the person or entity that, at the time of the taking, obtaining, or withholding, had the superior right to possession of the property. A general owner of property is a person who has title to it, whether or not that person has actual possession of it at the time. A special owner, such as a borrower or hirer, is one who does not have title but who does have actual possession or the right of possession of the property.

e. The taking, obtaining, or withholding of the property must be wrongful. As a general rule, if the taking or withholding is done without the consent of the other or the obtaining is done by false pretense, it is wrongful. It is not wrongful if the property is taken, withheld, or obtained through legal authorization or, generally, if done by a person or entity that has a right to the possession of the property either equal to or greater than the right of the one from who is in possession of the property.

f. A false pretense is a false representation of a past or existing fact. A false pretense may be made by means of any act, word, symbol, or token. The pretense must be in fact false when made and when the property is obtained and it must have been made knowingly false. A false representation made after the property is obtained is not a violation of Article 121, a larceny is committed when a person obtains the property through false pretense with the intent to steal.

g. The intent in larceny is to permanently deprive or defraud the owner of their property or to appropriate the property to the thief's own use or to the use of any person other than the owner. These intents are collectively called intent to steal. A larceny can still be committed if a person obtains another's property first and then forms the intent to withhold the property from return to its owner. For example, a larceny is committed if a person rents a vehicle and then later decides to keep it permanently by either failing to return it or uses it for a purpose not authorized by the terms of the agreement, even though at the time the vehicle was rented, the person intended to return it after signing an agreement.

h. Wrongfully engaging in credit, debit, or electronic transactions to obtain goods or money is an obtaining-type larceny by false pretense.

i. Theft of services may not be charged under larceny. See Article 134 (General Article – Obtaining Services Under False Pretenses) for further details.

j. The theft of multiple items from multiple owners, if done at essentially the same time and place, is considered a single larceny. For example, a suitcase containing several different owners' property that is stolen is still one specification of larceny.

k. Property can also be lost, mislaid, or abandoned, then recovered by a finder. There may or may not be a larceny or wrongful appropriation with respect to the property in those circumstances. In determining the question of larceny, the case agent should determine if there is any indication to ownership. If there is an indication of ownership and a reasonable effort to restore the property has not been made by the subject, then it can be a larceny. If the property is

abandoned, it cannot be the subject of larceny since the owner had relinquished all claims to it. It should be noted that that Government property in surplus storage or intended for disposal (i.e., DRMO) is not considered relinquished from U.S. government ownership.

27-3.4. Elements of Wrongful Appropriation. The elements of Wrongful Appropriation under the UCMJ are:

a. That the accused wrongfully took, obtained, or withheld certain property from the possession of the owner or of any other person;

b. That the property belonged to a certain person;

c. That the property was of a certain value, or of some value; and

d. That the taking, obtaining, or withholding by the accused was with the intent temporarily to deprive or defraud another person of the use and benefit of the property or temporarily to appropriate the property for the use of the accused or for any other person other than the owner.

27-3.5. Legal Discussion – Wrongful Appropriation

a. Wrongful appropriation requires the intent to temporarily (vice permanently) deprive the owner of their property, which was wrongfully taken, obtained or withheld by the accused. In most other respects, larceny and wrongful appropriation are identical.

b. While the wrongful appropriation of property of a value of more than $500.00 is not a major offense (felony type offense), it is a major offense if the property wrongfully appropriated is any motor vehicle, aircraft, vessel, firearm, or explosive.

c. Examples of wrongful appropriation include: taking another's vehicle without permission with the intent to drive it a short distance and then return it to the owner (this is also referred to as "Joyriding") or obtaining a service weapon by falsely pretending to be going onto guard duty with the intent to use it on a hunting trip and then later returning it. An inadvertent exercise of control over the property of another will not result in wrongful appropriation. For example, a person who fails to return a rented boat at the agreed time because the boat was inadvertently put aground is not guilty of wrongful appropriation.

27-3.6. Elements of Stolen Property: Knowingly Receiving, Buying, or Concealing. The elements of Knowing Receiving, Buying, or Concealing Stolen Property under the UCMJ are as follows:

a. That the accused wrongfully received, bought, or concealed certain property of some value;

b. That the property belonged to another person;

c. That the property had been stolen;

d. That the accused then knew that the property had been stolen; and

e. That, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces or was of a nature to bring discredit upon the armed forces.

27-3.7. Legal Discussion – Stolen Property: Knowingly Receiving, Buying, or Concealing

a. The actual thief is not criminally liable for receiving the property stolen (they are a principle to larceny). Actual knowledge that the property was stolen is required, for which circumstantial evidence is permissible. The property must have been received without justifiable excuse or purpose to be wrongful, for example it would not be "wrongful" to receive the stolen property in order to return it to the owner or for law enforcement to seize stolen property.

b. The term "wrongful" means that the property was received without the consent of the true owner or without justification or excuse. The term "received" means to acquire possession, care, custody, management, or control. The property must in fact be stolen, which essentially means the government must in effect prove two crimes; the larceny and the receiving.

c. In this crime, "knowledge" is used in the broadest sense; for example, if one believes the article was stolen or if he has definite suspicions, but declines to inquire/investigate further, he may be guilty of receiving stolen property. Knowledge is usually determined by inferences from all the circumstances surrounding the receipt of the stolen property. Lastly, the property must have some value (over $2,500.00) for NCIS jurisdiction and that, under the circumstances, the conduct of the accused was to the prejudice and good order and discipline of the armed forces.

27-3.8 Elements of Obtaining Services Under False Pretenses. The elements of Obtaining Services Under False Pretense under the UCMJ is as follows:

a. That the accused wrongfully obtained certain services;

b. That the obtaining was done by using false pretenses;

c. That the accused then knew of the falsity of the pretenses;

d. That the obtaining was with intent to defraud;

e. That the services were of a certain value; and

f. That, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces or was of a nature to bring discredit upon the armed forces.

27-3.9. Legal Discussion – Obtaining Services Under False Pretenses. This offense is similar to the offense of larceny and wrongful appropriation by false pretenses, except the object obtained

is services (e.g., cable or telephone service) rather than money, personal property, or other articles of value.

27-3.10. Elements of Military Property of the US: Sale, Loss, Damage, Destruction, or Wrongful Disposition. The elements of the Sale or Wrongful Disposition of US military property under the UCMJ are as follows:

a. That the accused sold or otherwise disposed of certain property;

b. That the sale or disposition was without proper authority;

c. That the property was military property of the United States; and

d. That the property was of a certain value.

27-3.11. Legal Discussion – Sale or Wrongful Disposition of U.S. Military Property. This offense is presented here in the context of the sale of military property that was stolen or wrongfully appropriated from the U.S. government. Military property is all property, real or personal; owned, held, or used by the armed forces of the United States. It is immaterial that the property, in the context of this crime, had been issued to the accused, someone else or even issued at all. The value of the property controls the maximum punishment which may be adjudicated (and therefore whether a felony crime or not). Retail merchandise of service exchange stores (e.g., Navy Exchange (NEX) stores) is not considered military property under this article.

27-4. INVESTIGATIVE PROCEDURE

27-4.1. Considerations

a. As previously indicated, an element of a major criminal offense may be related to an apparent misdemeanor. "Petty" larceny within a barracks, cubicle, or room may involve an unlawful entry (UCMJ Article 134) or possibly a housebreaking offense (UCMJ Article 130). See NCIS-3, Chapter 26 (Burglary) for further details.

b. Since the value of the property at the time of the theft is the major determining factor in accepting jurisdiction, the agent must carefully weigh the evidence concerning the value of the property. Paragraph 46c(1)(g) of the MCM contains specific guidance concerning the establishment of the value of government property and nonmilitary property. In general, if the stolen property is owned by the Government, the price list of an official publication at the time of the theft is admissible as evidence of its value; however, the property must be shown to have been in the condition upon which the value indicated in the official price list is predicated. As a general rule, value of other property is the legitimate market value at the time of the theft. If there is a conflict, general market value prevails. For example, a government computer purchased in 1995 for $500.00 may now be worth only $25.00.

c. Guidelines and definitions for subcategories within larceny are as follows:

(1) Appropriated Government Funds: Funds authorized by an act of Congress to incur an obligation for a specific purpose.

(2) Non-Appropriated Government Funds: These funds are separate and apart from funds recorded by the government or the General Accounting Office and usually involve funds set aside for the welfare, comfort or pleasure of military or civilian employees.

(3) Government Checks: In determining the value of negotiable instruments, such as checks, paragraph 46c(1)(g) MCM (2005), states: "writings representing value may be considered to have the value which they represented, even though contingently, at the time of the theft." For example if the check is made out for $500, then the value of the stolen property is $500.00. If the stolen check was in possession of the government (i.e. military) it would be a larceny of government property, but if the stolen government check had been issued to a person and it was in their control or possession at the time of the theft, the larceny is of personal property. Individuals suspected of larceny involving checks (government or personal) may also be potentially violating UMCJ Article 123 (Forgery) and/or their federal or state criminal law equivalents if the individual attempts to cash the checks.

(4) Larceny while on a military/government installation does not necessarily constitute a larceny of government property. Circumstances of larceny of personal property while on a military/government installation could include; Red Cross funds, coffee mess funds, vending machine funds, personal firearms, personal property in a barracks room, or contractor property or equipment.

(5) Ordnance: Subcategory 6R, Larceny - Ordnance, includes investigations pertaining to larceny or wrongful appropriation of government-owned firearms, ammunition, explosives, and other destructive devices. Antique, ceremonial, replica, or ornamental firearms that cannot be readily converted to expel a projectile are not considered ordnance related. Investigations normally will not be conducted on deactivated ordnance, dummy grenades, dummy practice bombs, small amounts of ammunition (e.g., small arms, 9mm), and artillery shell cases; however, the "sensitive" issue or hazard potential must be assessed in each investigation. Ordnance thefts in these areas must be left to the discretion of the SAC; the judicious assessment of the potential security problem or sensitive nature of the theft must be weighed. See section on Ordnance/Explosives Thefts or Losses below.

(6) Firearms: Based on Title II of the Gun Control Act of 1968 (National Firearms Act) 26 USC 5861 et. Seq,. the term firearm encompasses:

(a) Any weapon which will, or is designed to, or may be converted to expel a projectile by the action of an explosive;

(b) The frame or receiver of any such weapon;

(c) Any firearm muffler or firearm silencer;

(d) Any destructive device, i.e., explosives, bomb, grenade, mine, etc;

(e) Initiation/detonation devices, blasting caps, and detonation cord;

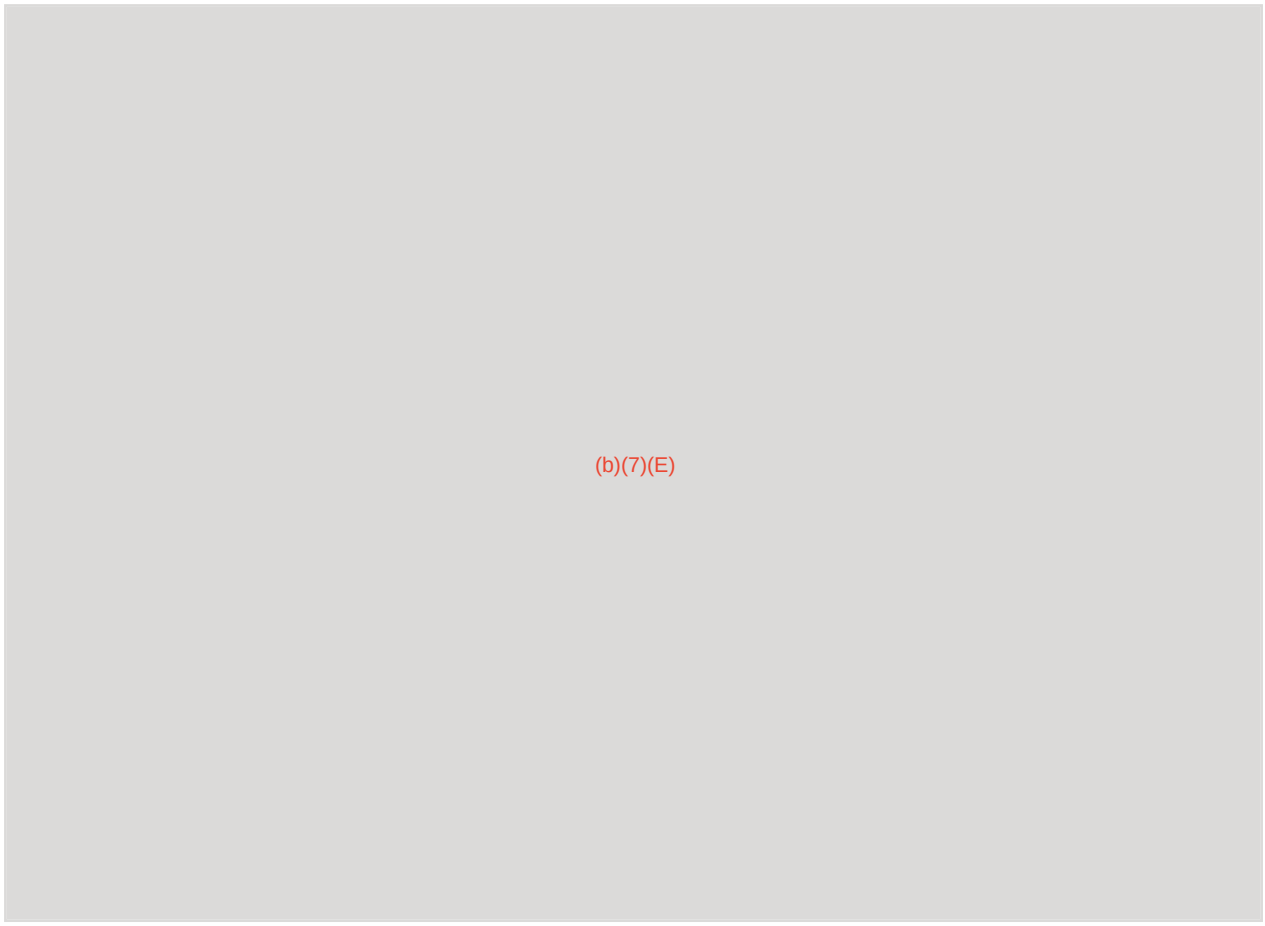
(f) Signal flares, pyrotechnic pistols, and line-throwing guns; and

(g) Ammunition.

(7) Vehicles: Includes private automobiles, motorcycles, trucks, vans, campers, and mobile homes. The theft of a vehicle on a military or government installation is a felony offense under the UCMJ, regardless of value.

27-4.2. Procedures

a. General larceny investigative procedures are, of course, dictated by the surrounding circumstances. As in all criminal investigations, general techniques such as crime scene search, collection and processing of evidence, latent print examination, photography, searches, surveillances, and interviews may be used. The techniques described below are particularly significant in perfecting a larceny case. All investigative effort must be directed to substantiate each element of the particular offense. General steps:



(b)(7)(E)

27-4.3. Ordnance/Explosive Thefts or Losses. In all larceny cases involving weapons or explosives (subcategory 6R), the NCIS special agent shall exercise extra caution in searches, interviews, arrests, and custodial interrogation of suspects. Notify the Federal Bureau of Investigation (FBI) and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), and NCISHQ regarding the theft of weapons, explosives, or ordnance. The following procedures should be followed in relation to ordnance, explosives, or weapons thefts:

(b)(7)(E)

If the weapon, ordnance, or explosives are recovered, then fax the Form 5400.5 previously submitted back to ATFHQ with the annotation “Amend – Recovered” added to the top of the form. The ATF local office should be notified of losses of firearms, ordnance, or explosives in the following categories:

(1) One or more missile or rocket rounds;

(2) One or more machine guns;

(3) One or more automatic fire weapons;

(4) Twenty-five or more manually operated or semi-automatic weapons;

(5) Ammunition (reportable incidents do not include losses known to have occurred during training). 40mm and smaller - 5,000 rounds or more. Only in the case of .38 caliber, report losses of 20,000 rounds or more.

(6) Ammunition that is larger than 40mm - five (5) rounds or more;

(7) Any fragmentation, concussion, or high explosive grenade, to include artillery or ground burst simulators, or any other type of simulator or device containing explosive materials;

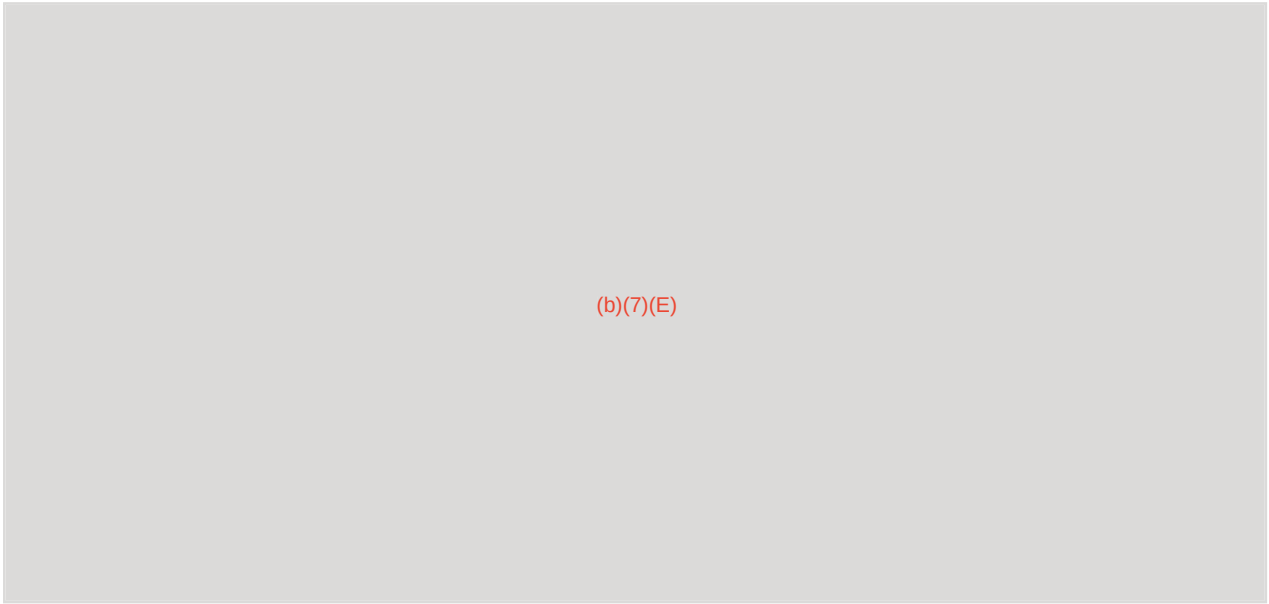
(8) One or more mines - anti-personnel or anti-tank;

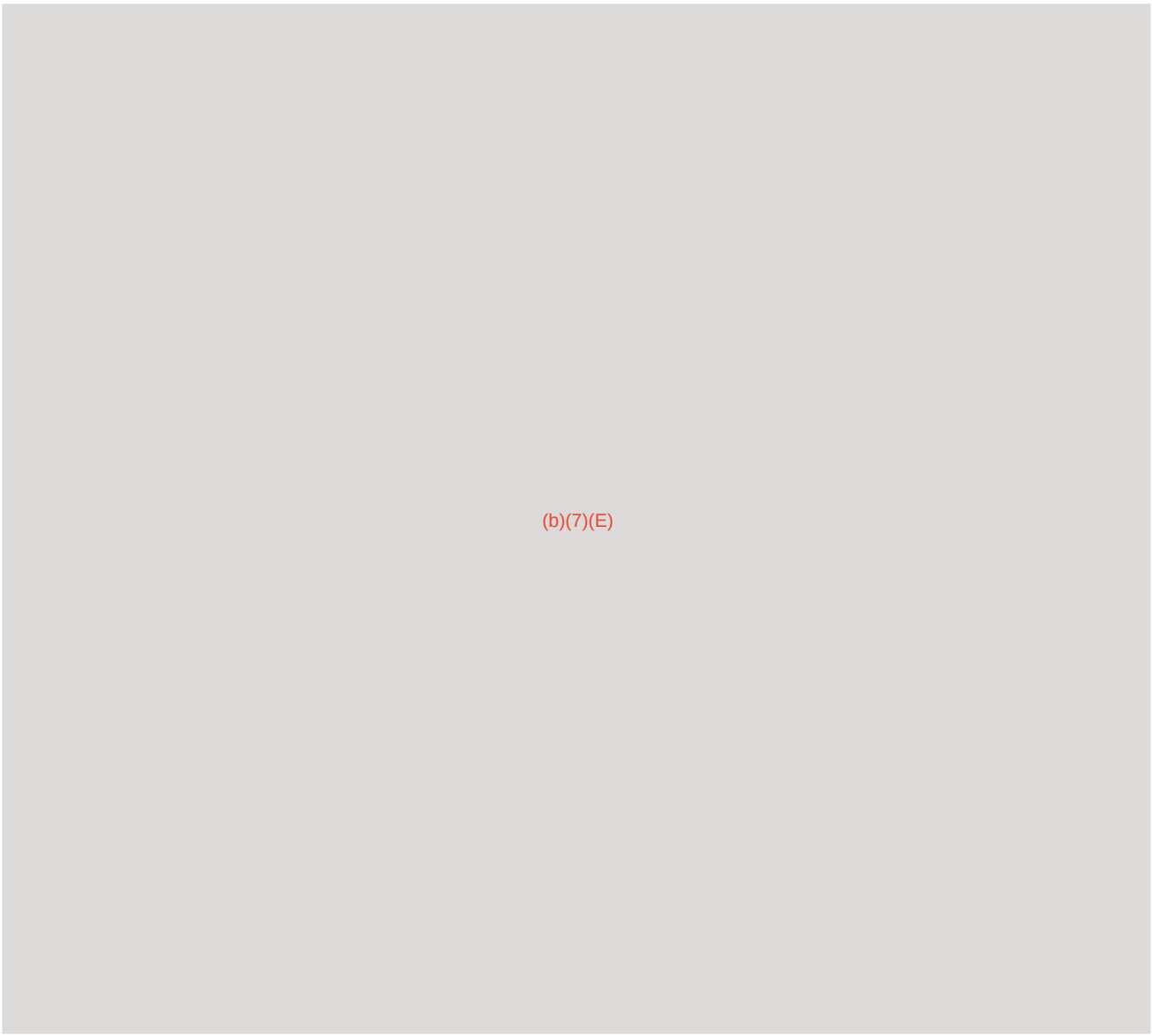
(9) Demolition explosives, including detonation cord, blocks of explosives (like C-4), and other explosives.

c. NCISHQ, both Code 0024 (Operational Support Directorate) and 0023 (Criminal Investigations Directorate), need to be informed immediately. If after hours, contact the Multiple Threat Alert Center (MTAC).

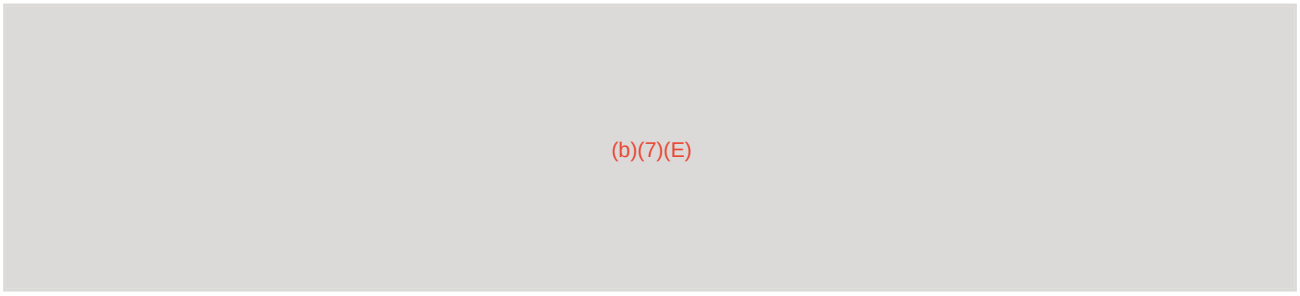
d. If appropriate, the local police department or sheriff's office should be informed of the theft or loss of firearms, ordnance, or explosives.

27-4.4. Investigating Ordnance/Explosive Thefts. When investigating losses or suspected larceny of firearms, ordnance, or explosives, the following should be kept in mind during the investigation.





27-4.5. OPNAVINST 5530.13C (26SEP03) “DON Physical Security Instruction for Conventional Arms, Ammunition, and Explosives (AA&E),” requires a thorough investigation to be made of missing, lost or stolen firearms, ordnance, and explosives to determine the circumstances and fix responsibility as appropriate. This instruction does not apply to privately-owned weapons and ammunition; which still may require an investigation by NCIS. Navy and Marine Corps units are instructed to promptly submit appropriate information relating to the theft or loss of firearms, ordnance, or explosives to the local NCIS office.



b. The cognizant NCIS office should make NCIC entries and also notify the Navy Registry (NAVSURFWARCENDIV Crane, IN, Code 4086), via NCISRU Crane, when applicable. If DON or other DoD weapons or explosives are recovered, NCIS should make the appropriate notifications in NCIC and the Navy Registry.

c. Should NCIS decline to investigate, then the NCIS office will notify the security officer or provost marshal, who will perform the investigation.

d. The Missing, Lost, Recovered or Stolen (MLSR) program has been eliminated in the Navy; however, the term "MLSR" may still be referred to by USMC and USN units in relation to AA&E thefts.

e. Per DoD Publication 5100.76-M (12AUG00) "Physical Security of Sensitive Conventional Arms, Ammunition, and Explosives," incident reports will be made to the Office of the Secretary of Defense in certain situations. The Director of Security, OASD(C3I), DASD(S&IO) shall be provided reports from the DON components who report significant incidents of confirmed theft or loss of AA&E. While this is generally the responsibility of the command, the case agent should be aware of the potential heightened visibility. The following shall be considered significant:

(1) One or more Category I or II missiles or rockets.

(2) One or more machine-guns.

(3) One or more automatic fire weapons.

(4) 25 or more manually operated or semi-automatic fire weapons.

(5) Over 5000 rounds of ammunition smaller than 40 mm.

(6) 20,000 rounds or more of .38 caliber.

(7) Five rounds or more of 40 mm and larger.

(8) Any fragmentation, concussion, or high explosive grenade.

(9) One or more mines (antipersonnel and antitank).

(10) Ten pounds or more of demolition explosives, including detonation cord, and blocks/sticks of explosives (C-4, dynamite, etc.).

(11) Armed robberies and attempted armed robberies of AA&E facilities.

(12) Forced entries or attempted forced entries into AA&E facilities.

(13) Evidence of terrorist involvement in the theft of AA&E.

(14) Incidents involving AA&E that cause significant news coverage, or appear to have the potential to cause such coverage.

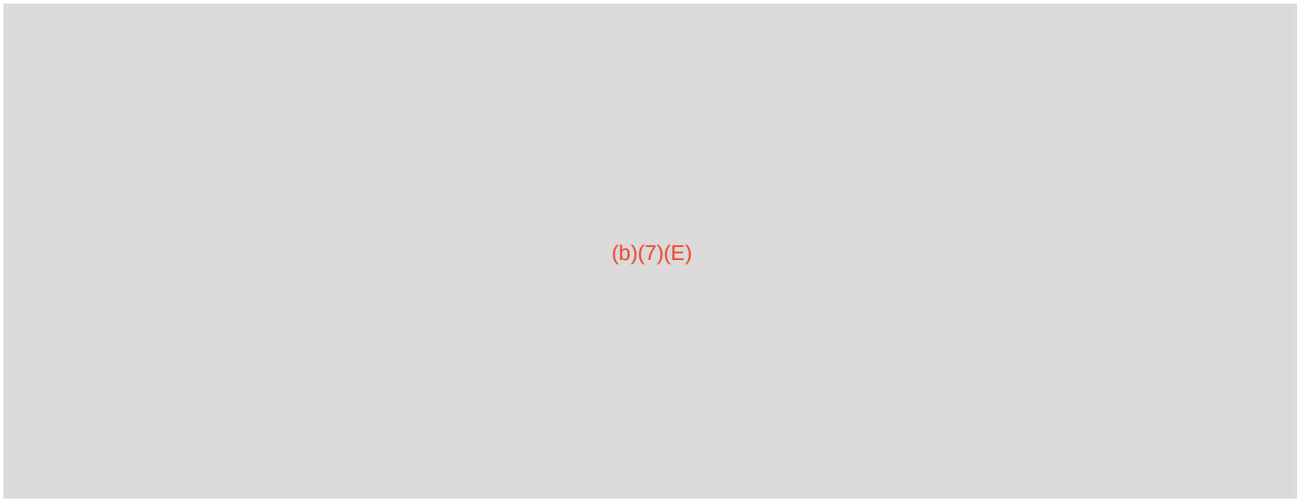
(15) Evidence of trafficking/bartering involving AA&E, illegal drugs, etc., regardless of the quantity of AA&E involved.

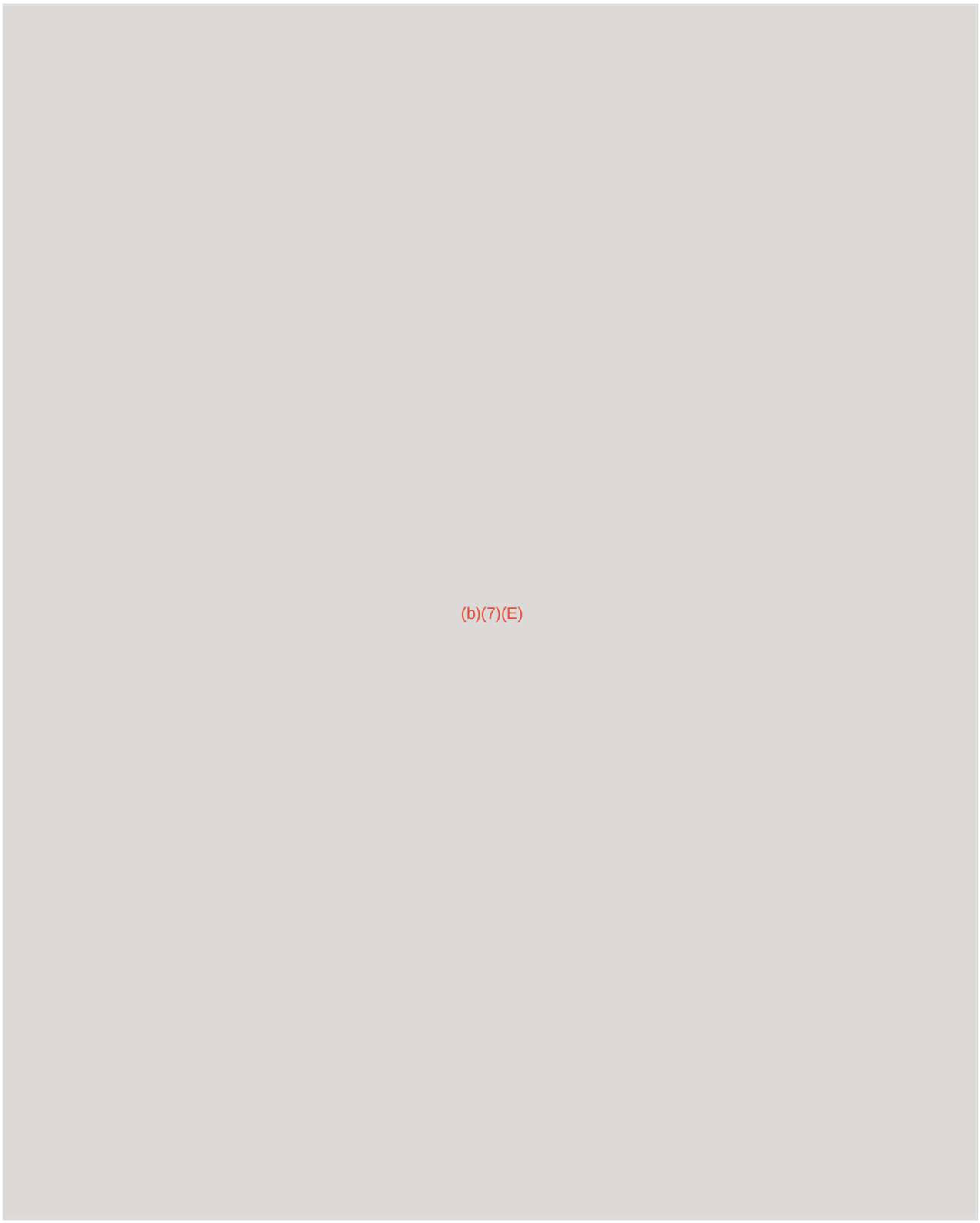
27-4.6. Auto Theft Investigation. Although there are many professional auto thefts in the United States, the majority of auto thefts investigated by NCIS fall into the category of Wrongful Appropriation, or "joyriding." Here the suspect steals the car for transportation, racing, or "borrows" the vehicle without the owner's consent. Other motives occur, such as car stripping or insurance fraud, but to a far lesser extent.

a. Auto Theft - General. The UCMJ, Article 121, is harsh in the penalty for vehicle thefts. The larceny of a vehicle, regardless of value, is punishable by five years confinement and Wrongful Appropriation, that is with the intent to "temporarily deprive," can be punished by two years confinement, also regardless of the vehicle's value. While NCIS initiates vehicle thefts aboard military installations (case categories 6S for government vehicle and 6V for a private vehicle), the NCIS special agent must be aware of the applicable Federal laws. The Interstate Transportation of Stolen Vehicles Act, Title 18, USC, Sections 2311-13, govern the Interstate Transportation of Stolen Vehicles. The Act describes the violations involved in the interstate transportation of stolen vehicles as well as the sale and receipt of stolen vehicles.

(1) Many requests for investigation arise when the vehicle larceny has occurred after trust. For example, when a vehicle which has either been borrowed from its owner or returned from a commercial agency is not returned at the agreed time. In such instances, investigation should be initiated upon receipt of a valid complaint.

b. Auto Theft - Preliminary Investigation. Basically, the preliminary investigation involves responding to the scene of the incident and conducting a personal interview with the complainant. The agent should get all the information necessary at this step and check the area for witnesses and establish the method of theft. Additionally:





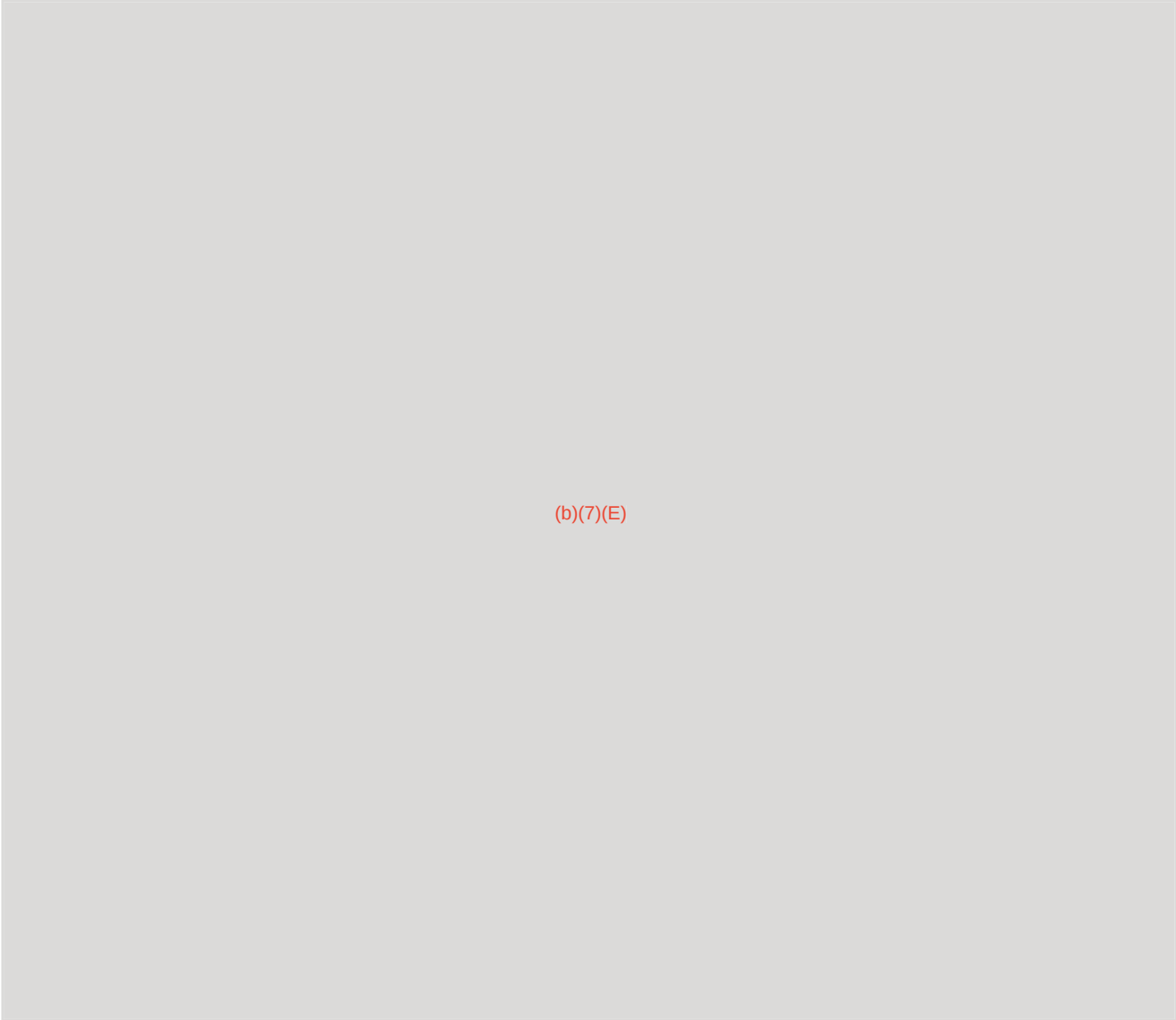
c. Processing a Recovered Car. If the auto has been found, NCIS agents should attempt to conduct an immediate inspection. If found by another police agency not serviced by NCIS, determine by NLETS/telephone if the local law enforcement agency can conduct a crime scene

search of vehicle. A police report should be solicited and documented as part of the NCIS investigation. Additionally, the following guidelines are suggested:

(b)(7)(E)

d. Examination of Burned Vehicles. Stolen vehicles are frequently found in a burned condition and the burning is almost always arson. The most common motive as mentioned above is insurance fraud, but cars are also burned to conceal other physical evidence or revenge on the owner. In any case, the following guidelines will assist the agent:

(b)(7)(E)



e. The tracing and identifying of vehicles is normally done by the FBI or the National Auto Theft Bureau (NATB). A tracing would include the manufacturer to the dealer to the last known owner. For additional information concerning the investigation of auto thefts, sources include the Department of Motor Vehicles, Highway Patrol or State Patrol, FBI, and NATB. The NATB is a non-profit organization sponsored by over 435 insurance companies. The NATB will provide a wide range of services nationwide at no cost, particularly in assisting in the identification and recovery of stolen autos or fire losses.

27-4.7. Wrongful Withholding (Embezzlement)

a. Of all the investigations in so-called white-collar crimes, embezzlement is one of the most difficult to conclusively prove. In this type of larceny, the accused comes into possession of the property or money lawfully, but the wrongful withholding may arise either:

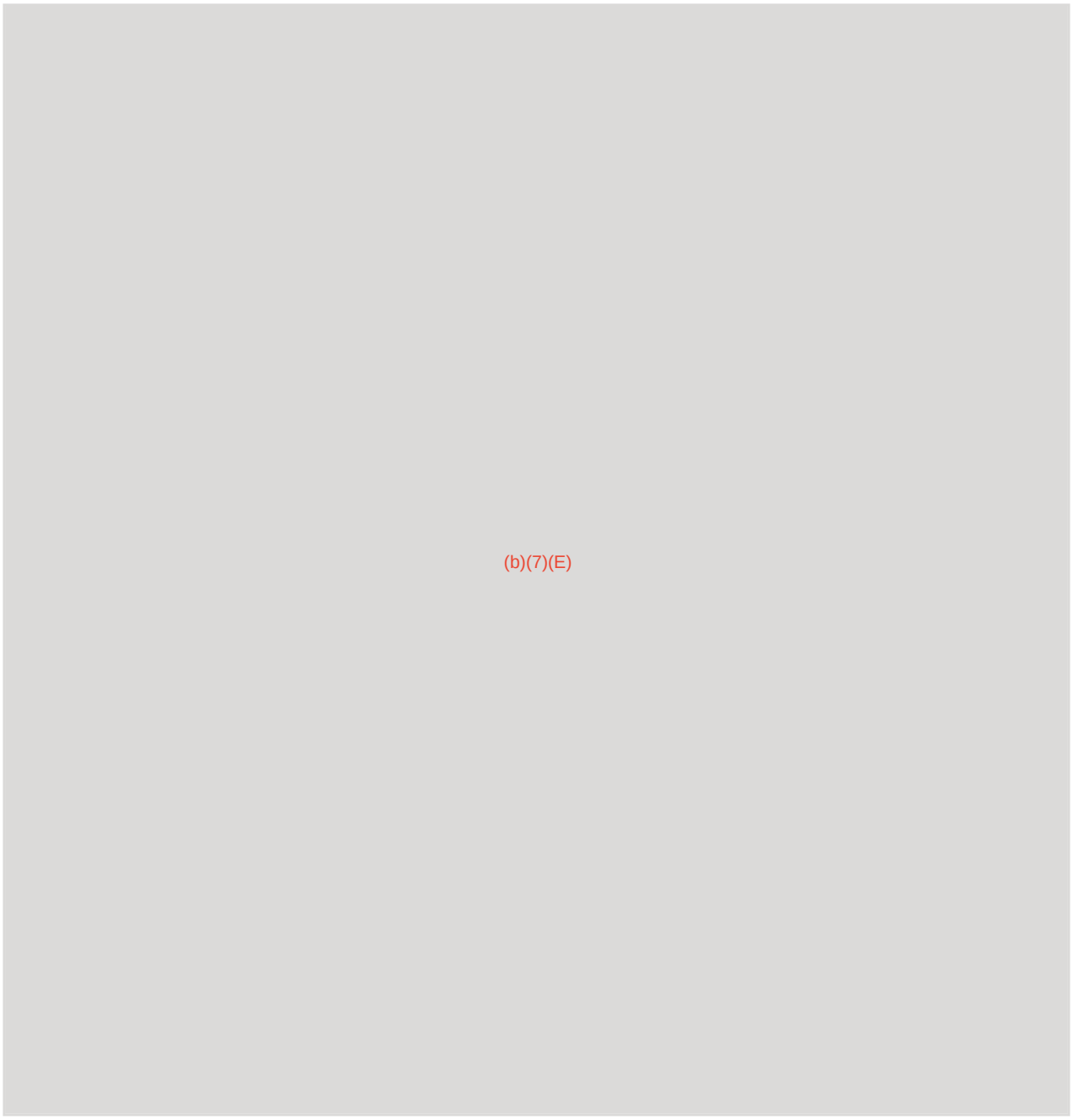
(1) As a result of a failure to return, account for, or deliver property to its owner when a return, accounting or delivery is due; or

(2) As a result of devoting the property to a use not authorized by its owner. Paragraph 46c(1)(b), MCM.

b. The "failure to return, account for, or deliver" type of larceny or "embezzlement" is typically committed by one having custody of funds; for example, a cashier at a Navy Exchange, ship's store clerk, or disbursing clerk. The agent must prove a corpus delicti; that is, that a crime did in fact occur. A failure or inability to account for the funds allows an inference of larceny, but a reasonable explanation may raise a doubt of guilt. Thus, the agent must concentrate on finding all explanations of missing funds. He must carefully examine inventory records as well as audit records.

c. Typically, after a surprise audit, the Command reports that the custodian has a "shortage" and the Command requests an investigation. The mere failure or inability, however, of a custodian to account for the funds does not in and of itself constitute larceny. The agent must prove the custodian stole the funds. He must find reasonable evidence that the custodian wrongfully converted the funds. The accused may be guilty of negligence or poor record keeping, but not larceny (remember intent is necessary here). Often times, larceny must be proved by circumstantial evidence. For example, a recent purchase of a new car with no adequate explanation of funds may help in the prosecution. The agent literally may have to negate the possibility that the accused could purchase an auto.

d. Thus, based upon the above brief discussion concerning the difficulty in proving the embezzlement case, the following basic guidelines are offered:



27-4.8. Investigations Involving Online/Internet Sales of Stolen Property. With the anonymity and ease of using the Internet to perform transactions and purchases, it has become a possible alternative to utilize services such as eBay or Craigslist to sell stolen items. Along with potential larceny or wrongful appropriation charges, this situation may also be a violation of UCMJ Article 134 (General Article) for the Sale or Wrongful Disposition of U.S. Military Property or Title 18 USC Section 2315 (Sale or Receipt of Stolen Goods, Securities, Moneys or Fraudulent State Tax Stamps). Depending on where the sale of the stolen goods occurs, state laws for the resale of stolen property may apply. Depending on the circumstances, the purchaser may be violating UCMJ Article 134 (General Article) for Knowingly Receiving, Buying, or Concealing Stolen Property.

a. eBay (www.ebay.com) is one of the largest online auction and sales website currently in operation. eBay allows individuals with accounts to post almost any item to be auctioned for by other visitors to the website. Anyone can get an account or login to get onto the site. Once an auction is completed, the money is transacted using another online service called PayPal (www.paypal.com) to transfer money from the purchaser to owner and the owner will usually mail the item purchased. The people involved will generally never meet physically or speak to each other, except through emails or online chat.

b. Craigslist (www.craigslist.org) is a popular locality-based online community for classifieds and forums, that can be used for many things such as sale of goods and services, social activities, etc. all for free. Site users can post information for free to sell items and the site is open for anyone to search for what ever they are looking for. Any transactions and communication between the owner and the purchaser are decided and agreed upon by the individuals.

c. For the investigation involving online sites, such as eBay and Craigslist, keep the following in mind:

(b)(7)(E)

d. There are other internet sites and services always coming online, eBay and Craigslist are only provided as examples of major web sites/services.

27-5. IDENTITY THEFT

27-5.1. General. Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain. Identity theft is simply the theft of identity information such as a name, date of birth, Social Security Number, credit card number, etc. The DON nexus to identity theft may be related to the protection of military personnel and their dependents or the prevention of duplication or production of false military identification. However, it is generally not the policy of NCIS to investigate individual missing or stolen military identification, vehicle decals or passes; unless it is an indication of a larger criminal or

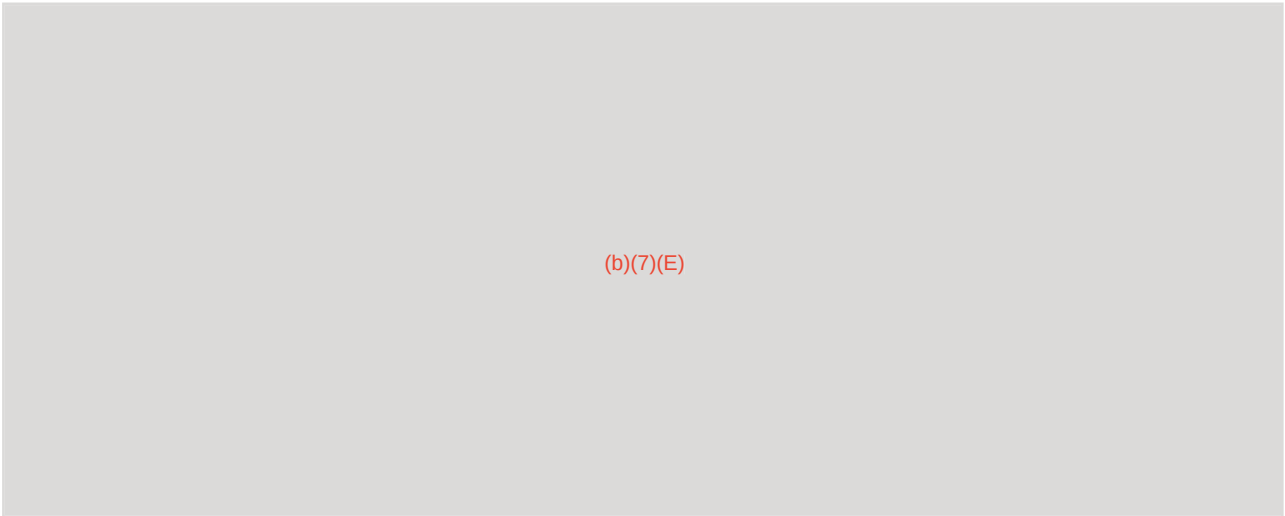
force protection matter. Some basic identity theft prevention information is provided on the NCIS public website (see http://www.ncis.navy.mil/info.asp).

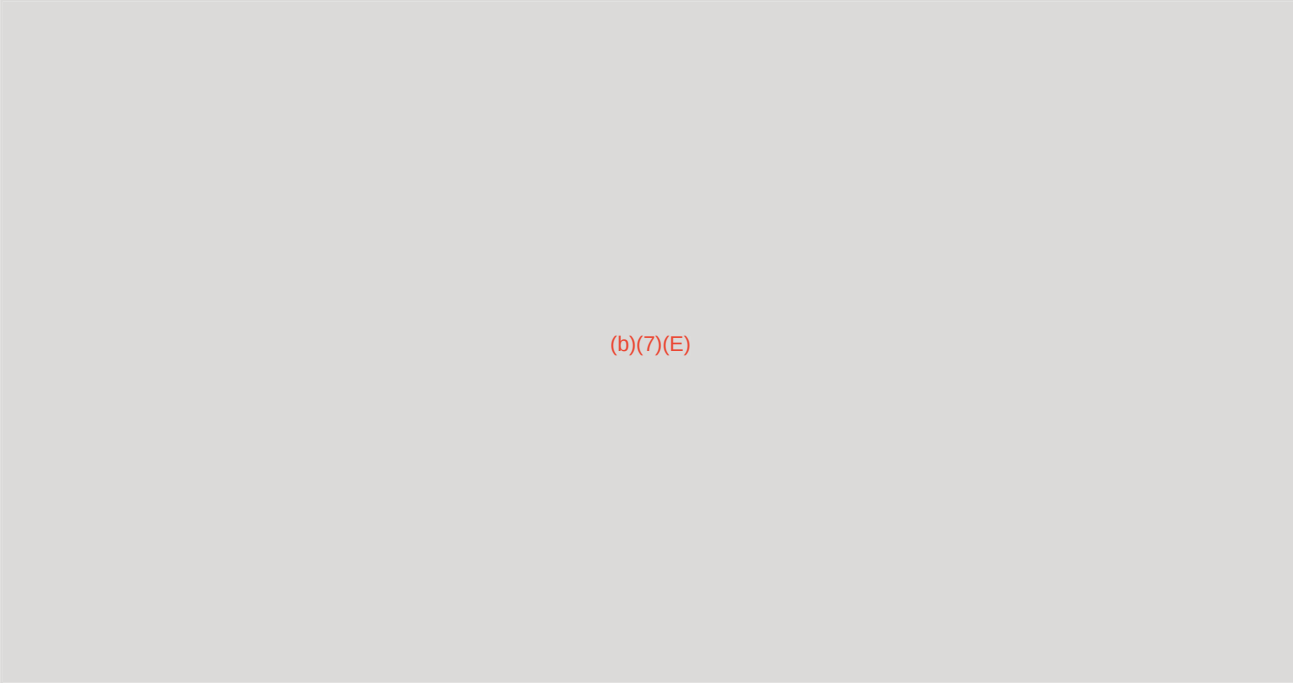
27-5.2. Criminal Methodology. Any activity in which identity information is shared or made available to others creates an opportunity for identity theft. Methods used to obtain identity information range from basic theft, organized schemes, bribery, deception, and "dumpster-diving." Victims of identity theft usually are not aware they are victims until they attempt to make a major financial purchase or receive a monthly bill (e.g., credit card bill). Identity theft occurs in many ways, such as carelessness on part of the victim, actual theft of personal information or items (e.g., purse, wallet, etc.), obtaining statements or other records the victim has thrown in the trash, deceptive online schemes, suspects misrepresenting themselves to the victim to acquire information, and malicious software affecting the victim's computer.

27-5.3. Investigating Identity Theft

a. Identity Theft and Fraud is one of the priorities of the Department of Justice, Department of Treasury, and the Federal Trade Commission (FTC) to pursue and prosecute. The FTC is responsible for receiving and processing complaints from people who believe they may be victims of identity theft and referring those complaints to appropriate entities, including the major credit reporting agencies and law enforcement agencies. The FTC does not have any criminal investigative authority; however, identity theft or fraud investigations are generally conducted by the FBI, the US Postal Inspectors Service, and the Secret Service.

b. To successfully investigate and prosecute an identity theft or fraud usually takes a mix of local, state, and federal officers working together to investigate and prosecute these multi-jurisdictional crimes. This is because generally the individual cases are "too small" for federal prosecution and "too large" or "too far abroad" for most local agencies to handle. Identity thieves try to commit their crimes over multiple jurisdictions and usually the victims don't realize they are victimized until weeks or months later, making it more difficult for an investigator. The following are some potential investigative steps to take in the investigation of an identity theft or fraud:





27-5.4. Laws Applying to Identity Theft

a. The primary federal identity theft statute is Title 18 USC Section 1028 (Fraud and Related Activity in Connection with Identification Documents, Authentication Features, and Information). The Identity Theft and Assumption Deterrence Act (1998) added Section 1028(a)(7) which criminalizes fraud in connection with the unlawful theft and misuse of personal identification information, regardless of whether the information appears or is used in documents. The penalties are as follows:

(1) Section 1028(b)(1)(D), provides a penalty of imprisonment of not more than 15 years when an individual commits an offense that involves the transfer or use of one or more means of identification if, as a result of the offense, anything of value aggregating $1,000.00 or more during a one year period is obtained.

(2) Otherwise, Section 1028(b)(2)(B) provides for imprisonment of not more than three years.

(3) Section 1028(b)(3) provides that if the offense is committed to facilitate a drug trafficking crime, or in connection with a crime of violence, or is committed by a person previously convicted of identity theft, the individual is subject to a term of imprisonment of not more than 20 years.

b. Most states have laws prohibiting the theft of identity information.

c. Identity theft may potentially be investigated under the following UCMJ Articles: Article 121 (Larceny), Article 124 (Forgery), Article 134 (General Article – False or Unauthorized Pass

Offenses), Article 134 (General Article – Obtaining Services Under False Pretense), and Article 134 (General Article – Mail: Opening, Taking, Secreting, Stealing or Destroying).

27-5.5. Legal Discussion – Identity Theft

a. "Means of identification" is defined (as per Title 18 USC Section 1028(d)(3)) as any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual. While it covers many different forms of personal identification, it specifically refers to Social Security numbers; date of birth; driver's license (and related identification); unique electronic identification numbers (e.g., ATM, personal identification numbers); telecommunication identifying information or access device (e.g., website login and password); and unique biometric data (e.g., fingerprints, voice print, retina identification).

b. Document-making devices used in creation of fraudulent identification are covered under Title 18 USC Section 1028(d)(1) and include any computers and software configured or primarily used for making identity documents.

c. Identity theft is often committed to facilitate other crimes, although it is frequently the primary goal of the offender. Other laws that may relate to identity theft include:

(1) Identification Fraud (Title 18 USC Section 1028(a)(1)-(6)),

(2) Credit Card Fraud (Title 18 USC Section 1029),

(3) Computer Fraud (Title 18 USC Section 1030),

(4) Mail Fraud (Title 18 USC Section 1341),

(5) Wire Fraud (Title 18 USC Section 1343),

(6) Financial Institution Fraud (Title 18 USC Section 1344),

(7) Mail Theft (Title 18 USC 1708), and

(8) Immigration Document Fraud (Title 18 USC 1546).

27-5.6. Responsibility to Victims of Identity Theft. While NCIS cannot investigate every suspected incident of identity theft, the agent does have a responsibility to assist the victim by at least providing advice as to assist the victim in how to deal with the theft of their identity. The agent can recommend to a victim of identity theft the following:

a. Contact the fraud departments of the three major credit bureaus; Equifax, Experian and TransUnion. Remind the victim to inform the credit bureau of the theft and request a "fraud alert" be placed on their file as well as a statement asking that the creditors call the victim before opening any new accounts.

b. Contact the security or fraud department of any creditors (e.g., credit card companies) of accounts in which the fraudulent activity occurred. Also, if financial information has been obtained by a suspect, the victim should immediately report the information to the financial institution.

c. Ask the victim to file a report with the local police or the police department where the identity theft occurred, if that can be determined. Remind the victim to get a copy of the police report as this may be needed to provide to creditors as proof of the theft.

d. Recommend the victim to go to the FTC website (www.ftc.gov) for more assistance and possibly file a complaint through the FTC.

e. Certain situations may require additional actions by the victim, such as:

(1) Identity theft involving mail should be reported to U.S. Postal Service.

(2) If investments or securities are involved, then the Securities and Exchange Commission should be contacted.

(3) Identity theft involving passports should be reported to the U.S. State Department.

(4) Identity theft of Social Security Numbers should be reported to the Social Security Administration.

(5) Identity theft of immigration documents should be reported to Bureau of Immigration and Customs Enforcement (ICE).

(6) Identity theft involving driver's licenses should be reported to the state's Department of Motor Vehicles (DMV).

Pages 783 through 784 redacted for the following reasons:
- -
(b)(6), (b)(7)(C), (b)(7)(E)
(b)(7)(E)

CHAPTER 28
TITLE: CRIMES AGAINST PROPERTY-OTHER (CATEGORY 6)
POC: CODE 23A
DATE: FEB 10

28-1. DISCUSSION

28-1.1. General. This chapter provides direction and discussion for the investigation of property related crimes not directly covered in other chapters of the NCIS-3. The case categories covered in this chapter are:

a. 6C – Blackmarketing,

b. 6G – Counterfeiting,

c. 6L – Postal,

d. 6M – Customs, and

e. 6X – Special Inquiry.

28-1.2. NCIS Investigative Responsibility. If NCIS investigates any of the crimes described in this chapter and when logical to the investigation, a detailed crime scene examination should occur, to include photographs, diagrams/sketches, evidence collection, and taking any victim and/or witness statements. Attempts should be made to employ forensic techniques as appropriate.

a. If an NCIS investigation is opened on any of the crimes described in this chapter, liaison with the local security force and/or police departments of adjacent communities and/or federal law enforcement entities should occur. Any police reports or incident reports made by other law enforcement entities should be requested as part of the investigation.

b. The investigating agent should obtain written statements from victims, pertinent witnesses, and suspects.

28-1.3. Criminal Intelligence. In some of the crimes discussed in this chapter there may not be enough evidence, information, or an identifiable suspect to open an investigation, such as the receipt of a single counterfeit bill. However, there may be potential criminal intelligence value in these

seemingly minor criminal offenses. When possible, investigating agents should provide a report of Information (ROI) (INFO) criminal intelligence report on singular violations or those situations when a full investigation is not initiated. The reports should be sent to NCISHQ Code 25B (MTAC Threat Analysis Division) and Code 25A3 (Criminal Intelligence). Special agents should ensure compliance with Department of Defense (DoD) Directive 5200.27 (Acquisition of Information Concerning Persons and Organizations Not Affiliated with the DoD) in regard to collecting information on U.S. persons.

28-2. CRIMINAL LAW/AUTHORITY/JURISDICTION

28-2.1. Criminal Law.

a. Uniform Code of Military Justice (UCMJ). This chapter examines several crimes that are potentially violations of the UCMJ, which are as follows:

Article 103 – Captured or Abandoned Property
Article 108 – Military Property of the US (Sale, Loss, Damage, Destruction, or Wrongful Disposition)
Article 134 – General Article (False or Unauthorized Pass Offenses)
Article 134 – General Article (Mail: Taking, Opening, Secreting, Destroying, or Stealing)
Article 134 – General Article (Public Record: Altering, Concealing, Removing, Mutilating, Obliterating, or Destroying)
Article 134 – General Article (Stolen Property: Knowingly Receiving, Buying, or Concealing)
Article 92 – Failure to Obey an Order or Regulation

All of the violations discussed in this chapter should be given consideration for attempts and conspiracies.

b. Federal Laws/US Code (USC). Crimes of this category are potentially violations of Title 18 USC Chapters:

25 – Counterfeiting and Forgery
27 – Customs (which includes Smuggling)
63 – Mail Fraud (which includes Wire Fraud)
83 – Postal Service
95 – Racketeering
96 – Racketeer Influenced and Corrupt Organizations
103 – Robbery and Burglary
113 – Stolen Property

See the USC for specific and most current information. Violations within the USC should be considered for attempts and conspiracies. Crimes in this category which occur in federal jurisdiction, which are not directly covered under federal law but are violations under local/state law, may be potentially investigated though the Assimilative Crimes Act, Title 18 USC Section 13.

c. State Criminal Law. Depending on jurisdiction and/or victim/suspect of crimes of this category (i.e., non-military personnel or government property), appropriate state penal code may apply.

28-2.2. NCIS Authority. NCIS authority and jurisdiction to investigate these categories of offenses are derived from SECNAVINST 5430.107. DoD Directive 5525.07 implements the Memorandum of Understanding (MOU) between the Department of Justice and the DoD criminal investigative organizations. This MOU provides policy and guidance for criminal investigations when both departments have jurisdiction. See NCIS-3, Chapter 1 (Authority, Jurisdiction, Scope) for further explanation.

28-2.3. NCIS Responsibility. Per SECNAVINST 5430.107, NCIS has the primary responsibility for liaison between law enforcement entities and Department of the Navy (DON) elements for the purposes of investigations. Several of the crimes discussed in this chapter may fall under the primary jurisdiction of another federal agency (e.g., counterfeiting of U.S. currency is investigated by the U.S. Secret Service (USSS)).

28-3. BLACKMARKETING (6C)

28-3.1. General. Investigated under case subcategory 6C, blackmarketing is the unlawful trafficking in commodities or currency and can exist in foreign countries or in the United States. Blackmarketing is a type of economic activity that takes place outside of government-sanctioned channels. Blackmarket transactions typically occur as a way for participants to avoid government price controls or taxes, or conducting transactions "under the table." The blackmarket is also the means by which illegal substances or products - such as illicit drugs, firearms or stolen goods - are bought and sold. From an agent viewpoint, the investigation of small time blackmarket activities is a difficult, often fruitless assignment. It must be realized, however, that all blackmarket activities should be investigated in the interest of suppressing crime, reducing possible terrorist financing, and developing information leading to the discovery of sources of blackmarket materials. The solving of a relatively minor case may lead to ringleaders involved in criminal or terrorist enterprises. Blackmarketing revenue has been used by individuals and groups to fund terrorist activities around the world.

a. Discussion – Blackmarketing.

(1) Blackmarketing. The unlawful exchange of commodities or currency in violation of price, priority, or rationing laws or of pertinent regulations. Persons or groups engaged in such activity may be classed as:

(a) Systematic Activity. These persons are organized into groups to carry on planned blackmarket operations. This category also includes individuals who are not members of blackmarket organizations, but who habitually engage in planned blackmarketing activities. It should be noted that profits from blackmarket activity may be used for personal gain or possible terrorist funding.

(b) Occasional Activity. These persons engage in blackmarketing activities on a sporadic or

opportunistic basis. Such persons are not normally members of an established blackmarketing ring.

(2) Source. A facility or location where items are diverted from authorized channels into the blackmarket; it can also be an individual who diverts items into the blackmarket. This individual may be a "fence."

(3) Transporter. This individual accomplishes the physical move of blackmarket items from one location to another. He/she may or may not be a member of a blackmarket ring, and may or may not be knowingly transporting blackmarket materials.

(4) Blackmarket Ring. A group of persons banded together for the purpose of planning and conducting blackmarket activities. Elements of such a ring may be so organized as to preclude one member, with the exception of the leader, from knowing all the other members.

b. Fences. A "fence" is a person who receives and sells stolen goods. The fence, who is a type of specialized criminal, earns a living by buying and reselling stolen merchandise by acting as a middleman for thieves and dealers. Dealers can include legitimate businesses, such as auction houses, collectors, merchants, etc. The fence operation can be run out of a location, or through agreements, or online (e.g., eBay). Fencing operations, depending on the circumstances, can be investigated under Blackmarketing (6C), Special Inquiry (6X), or Larceny (Ordnance – 6R, Government – 6S, or Personal – 6T; see NCIS-3 Chapter 27 (Larceny) for further detail).

(1) Professional Fences. These are individuals who have developed relationships with the thieves (suppliers), businessmen (dealers), law enforcement and others in the community.

(2) Non-professional Fences. These include individuals who may be merchants who integrate stolen property into their inventory or inform burglars about what to steal; they may also barter stolen goods for services or approach strangers with "great deals."

c. Legal Considerations – Blackmarketing. As the need arises, laws and regulations pertaining to price ceilings, priorities, taxation, and rationing are promulgated and published by proper authority. Special agents investigating allegations of blackmarketing must acquaint themselves with the provisions of such laws and regulations. Most of these laws and regulations are created to prevent the following:

(1) Loss of tax revenue through illegal trafficking.

(2) Loss of income by producers, suppliers, and retailers engaged in legitimate commercial enterprise.

(3) Corruption of public officials.

(4) Added cost in replacing military supplies and equipment that have been diverted into blackmarket channels, and lack of such supplies and equipment when needed for mission performance.

(5) Obligation against the United States to honor dollar instruments that have been purchased with blackmarket profits.

(6) Blackmarket activities, which can often be a precursor to the commission of other related crimes.

d. Dollar Instruments. Dollar (or cash) instruments are financial instruments whose value is determined directly by markets. They can be divided into securities (which are readily transferable) and other cash instruments, such as loans and deposits. Examples of securities are bank notes, treasury checks, bonds, and common stocks. Incidents involving negotiable dollar instruments on the blackmarket should receive special consideration because they often result in a direct dollar loss to the United States. Reports should be made to the appropriate law enforcement agency indicating that dollar instruments are being illegally diverted into channels that do not serve the interest of the United States.

e. Conditions Conducive to Blackmarketing. Blackmarketing may exist anywhere, domestically or internationally, provided this activity is profitable. Conditions conducive to blackmarketing include, but are not limited to:

(1) A breakdown in a country or location's economic structure.

(2) A scarcity of certain commodities that are in great demand.

(3) The availability of those commodities in demand on the blackmarket at commissaries, exchanges, and government sales stores.

(4) A price differential between items on the blackmarket and the same items on the open market.

(5) A failure of personnel at commissaries, exchanges, government sales stores, warehouses, and depots to keep adequate records of sales and distribution of commodities and to take necessary security measures to protect these commodities in storage.

(6) The capability to use the mail or other authorized means for the transport of commodities in demand on the blackmarket.

(7) A failure of proper authorities to publish appropriate laws, orders, and regulations to suppress or prevent blackmarketing.

(8) A failure to enforce existing laws, orders, and regulations and to punish known offenders. A lack of punishment can have a demoralizing effect on law-abiding citizens.

28-3.2. Legal Considerations. This section discusses possible UCMJ violations that may be used in blackmarketing investigations. Consult with the proper legal authority in the jurisdiction of the investigation for additional discussion of legal considerations.

a. Article 103 – Captured or Abandoned Property.

(1) All captured or abandoned public property taken from the enemy for the service of the United States shall be secured, notice given and turned over to the proper authority without delay.

(2) Any person who fails to carry out these duties or buys, sells, trades, or in any way deals in or disposes of captured or abandoned property, whereby he receives or expects any profit, benefit, or advantage to himself or another person directly or indirectly connected with himself is in violation of this article.

(3) Any person engaging in looting or pillaging is in violation of this article.

(4) The individual violations of this article are as follows:

(a) Failing to secure public property taken from the enemy,

(b) Failing to report and turn over captured or abandoned property,

(c) Dealing in captured or abandoned property, and

(d) Looting or pillaging.

(5) Nature of Property. In regard to this article, failing to secure property taken from the enemy involves only public property. Immediately upon its capture from the enemy, public property becomes the property of the United States. Neither the person who takes it nor any other person has any private right in this property.

(6) Looting and Pillaging. This refers to unlawfully seizing or appropriating property which is located in enemy or occupied territory.

b. Article 108 – Military Property of the US (Sale, Loss, Damage, Destruction, or Wrongful Disposition).

(1) Any person without proper authority who:

(a) Sells or otherwise disposes of;

(b) Willfully or through neglect damages, destroys, or loses; or

(c) Willfully or through neglect suffers to be lost, damaged, sold, or wrongfully disposed of, any military property of the U.S. shall be in violation of this article.

(2) The individual violations of this article are as follows:

(a) Selling or otherwise disposing of military property;

(b) Damaging, destroying, or losing military property; or

(c) Suffering military property to be lost, damaged, destroyed, sold, or wrongfully disposed of.

(3) Military Property. This refers to all property, real or personal, owned, held, or used by one of the armed forces of the U.S. It is immaterial whether the property has been issued to the accused, to someone else or even issued at all. Retail merchandise of the Navy Exchange (NEX) or Marine Corps Exchange (MCX) is not military property under this article.

(4) To Suffer. This means to allow or permit.

c. Article 134 – General Article (Stolen Property: Knowingly Receiving, Buying, or Concealing). See NCIS-3, Chapter 27 (Larceny) for further discussion.

(1) The actual thief is not criminally liable for receiving the stolen property; however, he is a principal to the larceny (see NCIS-3, Chapter 27 (Larceny)). When the accused is not the actual thief, they may be found guilty of knowingly receiving the stolen property; however, they cannot be guilty of both larceny and receiving stolen property.

(2) Knowledge. The accused must have actual knowledge that the property was stolen. This knowledge may be proved through circumstantial evidence.

(3) The value of the property is relevant to the crime. Property with a value greater than $500.00 is a felony.

d. Article 92 – Failure to Obey an Order or Regulation. This article of the UCMJ is in relation to violating Navy Regulations or instructions prohibiting such acts.

28-3.3. Liaison. Agencies or entities with which the investigating agent should maintain liaison for cooperation purposes include, but are not limited to:

a. Base Police/Base Police Investigative Division, USMC Military Police, and CID. This is especially true in a foreign port or location.

b. Military intelligence and other intelligence and other military criminal investigative agencies. Examples include Air Force OSI, US Army CID, Office of Naval Intelligence (ONI), and Marine Corps Intelligence Activity (MCIA).

c. NEX and MCX Systems.

d. Navy, Army, Air Force Postal Service and the U.S. Postal Inspection Service (USPIS).

e. The General Services Administration (GSA).

f. Relief and economic assistance agencies.

g. Banks; quasi-military and civilian.

h. Civilian police.

i. Local tax offices.

j. Local chambers of commerce.

k. American Express Company branches.

l. Pawnbrokers.

m. Officers, NCO, Chiefs' and enlisted clubs and messes.

n. The US Department of Justice (to include the FBI and DEA).

o. The Internal Revenue Service (IRS).

28-3.4. Sources of Blackmarketing Information. Sources of information include, but are not limited to:

(b)(7)(E)

b. Anonymous Tips. Information may be received through anonymous telephone call or letter. Various motives prompt individuals to give information of this nature; consequently, such information should be viewed with suspicion until proven valid. Nevertheless, each such tip should be checked before it is dismissed.

c. Apprehended Military Persons and/or Arrested Persons. The interrogation of persons apprehended/arrested for blackmarketing or other offenses may provide information on known or suspected blackmarket operators or may reveal new suspects.

d. Reports of Shortages or Thefts. The screening of reports submitted concerning supply shortages or thefts may produce important investigative information. Because of the possible transfer or relocation of personnel involved, these reports should be screened promptly and any indicated leads should be checked out as soon as possible. Experience will indicate which missing supplies are likely to appear on the blackmarket.

e. Postal Officials. Upon official request, postal authorities may provide information relative to the purchase of money orders. Such information may reveal that purchasers had more money than they might normally be expected to have, and thus, may provide reasonable grounds for further investigation.

f. Supply and Maintenance Agencies and Units. The agencies and units of the supply and maintenance services normally handle or stock many commodities that may make their way onto the blackmarket. Both the personnel and the records of these agencies may be valuable sources of information as to types and amounts of missing supplies and places where these commodities might have left authorized channels of distribution.

g. Local Civilian Employees of the Navy. If local civilian employees are encouraged to report any irregularities they observe, they may provide extensive and valuable information. Employees may be encouraged to make such reports by pointing out to them that blackmarketing activities are detrimental to the economy of their country.

(b)(7)(E)

i. Naval Audit Service. In the course of its activities, the Naval Audit Service may detect irregularities that may be linked with blackmarketing activities.

j. Commissaries, Exchanges, and Sales Stores. Personnel employed at these places may be a valuable source of information in that they may detect irregularities on the part of fellow employees and the excessive sale of blackmarketable commodities to certain individuals. Some exchanges have their own security personnel who can also be a source of pertinent information.

k. Finance Offices. Information on the amounts of money that military personnel have exchanged through finance offices may be helpful in detecting individuals who have more money than they should legally possess.

(b)(7)(E)

m. Merchants. Since merchants are concerned with the buying and selling of commodities, they may know about commodities that are being procured from the blackmarket. They may be able to provide the names of individuals who have such commodities for sale.

(b)(7)(E)

28-3.5. Investigative Concerns. Investigation of blackmarket activities involves the standard investigative procedures employed in criminal cases, such as interviewing witnesses, interrogating

suspects, surveillance, collection and preservation of evidence, and obtaining statements and confessions. Some important factors to seek are:

(b)(7)(E)

28-3.6. Investigator Concerns. (b)(7)(E) (b)(7)(E) The need for skilled investigators is accentuated by the fact that sound judgment and extreme caution are required to preclude a premature action in bringing the investigation to a close. An agent must resist the temptation to apprehend the suspect prematurely for possession of a minimal amount of contraband when it is known that the suspect deals in much larger amounts and is associated with local nationals.

a. Pertinent information regarding blackmarketing supplied by local law enforcement agencies and close liaison with such agencies is paramount if NCIS is to exercise control over blackmarketing in a naval area. The agent, however, must be constantly aware that members of the local law enforcement agency could potentially be involved in blackmarket operations that emanate from the naval facility.

28-3.7. Blackmarket Initiative Operations. In order to ensure the most efficient utilization of resources, initiative blackmarket operations targeting non-DoD personnel will not be undertaken by NCIS components absent a specific request by host country officials. This request will contain the identity of the requesting official, the objectives of the operation, and assurance from the host country law enforcement and judicial officials (fully identified) that violators will be prosecuted to the fullest extent of the law. (b)(7)(E) (b)(7)(E) (b)(7)(E) See NCIS-3, Chapter 9 (Crime Reduction Operations) for more information on initiative operations.

28-4. COUNTERFEITING (6G)

28-4.1. General. Investigated under case category 6G, counterfeiting of currency, coins, or other

U.S. Government obligations victimizes thousands of citizens. The problem of controlling this illegal activity is aggravated by technological advances in printing and by reproduction machines that enable persons with little or no skill to engage in counterfeiting. The mobility of the modern criminal permits him to pass the counterfeit currency hundreds of miles from its source. A counterfeiter can duplicate any obligation or document that will afford them profit or gain. Some examples are: bonds, money orders, official seals, stamps, and identification cards.

a. This case category also includes the counterfeiting of official documents, military identification, "pass and ID" decals, and driver's licenses. Examples of typically counterfeited official documents include passports, immigration documents, and Social Security cards. Depending on the document, primary jurisdiction for investigation may be with another law enforcement agency.

b. "Blank" Military Identification Cards or Vehicle Decals. Stolen "blank" military or civilian identification cards (e.g., Common Access Cards (CAC)) and vehicle decals (i.e., "pass and ID" decals) may be a significant security issue or potentially used to commit other offenses. The theft of "blank" identification cards or decals should be investigated under the Special Inquiry (6X) subcategory. N (b)(7)(E) (b)(7)(E) (b)(7)(E) The initiation of an investigation regarding theft of "blank" ID cards or decals will be left to the discretion of the cognizant NCIS office when a minimal number of cards or decals are involved. However, it is generally not the policy of NCIS to investigate individual missing or stolen military identification, vehicle decals or passes; unless it is an indication of a larger criminal or force protection matter. "Blank" military identification and decals that have been altered with fraudulent or legitimate personal information should be investigated as counterfeiting (6G).

c. Identity Theft. Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain. Identity theft is investigated under the crime category of Larceny, see NCIS-3, Chapter 27 (Larceny) for further explanation. Use of stolen personal identification information to alter an identification document/card (e.g., CAC) or decal can be investigated for counterfeiting (6G) or larceny (Chapter 27).

28-4.2. Definitions.

a. Counterfeiting. To criminally forge or print a false copy of money, bonds, or other valuable documents, intending to profit from the falsity.

28-4.3. Jurisdiction. When evidence of counterfeiting U.S. obligations and securities (currency, U.S. Treasury checks, U.S. postage stamps) is discovered in the United States or its territories, the United States Secret Service (USSS) has primary jurisdiction and should be immediately informed. In the absence of USSS agents in overseas areas, NCIS will assume investigative responsibility and provide the nearest USSS office a copy of the counterfeiting investigation report; as well as informing the local U.S. Embassy of the counterfeiting. NCIS should concurrently investigate with foreign authorities when a foreign institution, such as a bank or financial facility authorized to deal

in foreign exchange, has been victimized by counterfeit U.S. currency. In the absence of logical substantive leads, an investigation should not be initiated; however, an ROI (INFO) should document the matter. Copies of the report should be forwarded to NCISHQ Code 25A3 (Criminal Intelligence).

a. Counterfeiting of other official documents may fall under the primary jurisdiction of different law enforcement agencies. NCIS special agents should immediately inform the appropriate agency of the possible counterfeit document. In overseas locations, the United States Embassy should be informed. The following are documents that may typically be counterfeited and their responsible agency:

(1) Immigration documents – Bureau of Immigration and Customs Enforcement.

(2) Social Security cards – Social Security Administration Inspector General.

(3) Passports and visas – Diplomatic Security Service.

(4) Driver's license, state identification and birth certificates – State bureau of investigation and/or the local police department or county sheriff.

28-4.4. Legal Considerations. This section discusses possible UCMJ violations that may be used in counterfeiting investigations. Consult with the proper legal authority in the jurisdiction of the investigation for additional discussion of legal considerations.

a. Article 134 – General Article (False or Unauthorized Pass Offenses).

(1) In general, the terms "military or official pass, permit, discharge certificate, or identification card" includes all documents issued by any governmental agency for the purpose of identification and copies thereof.

(2) The possession or use with the intent to defraud or deceive is a felony. The making, altering, counterfeiting, tampering with, or selling is a felony. All other cases involving this article are misdemeanors; such as, possession of a false identification card <u>without</u> the intent to deceive.

b. Elements of False or Unauthorized Pass Offenses. The following are the elements of Article 134 under the UCMJ:

(1) Wrongful making, altering, counterfeiting, or tampering with a military or official pass, permit, discharge certificate or identification card.

(a) That the accused wrongfully and falsely made, altered, counterfeited, or tampered with a certain military or official pass, permit, discharge certificate, or identification card; and

(b) That, under the circumstances, the conduct of the accused was to the prejudice of the good order and discipline in the armed forces or was a nature to bring discredit upon the armed

forces.

(2) Wrongful sale, gift, loan, or disposition of a military or official pass, permit, discharge certificate, or identification card.

(a) That the accused wrongfully sold, gave, loaned, or disposed of a certain military or official pass, permit, discharge certificate, or identification card;

(b) That the pass, permit, discharge certificate, or identification card was false or unauthorized;

(c) That the accused then knew that the pass, permit, discharge certificate, or identification card was false or unauthorized; and

(d) That, under the circumstances, the conduct of the accused was to the prejudice of the good order and discipline in the armed forces or was a nature to bring discredit upon the armed forces.

(3) Wrongful use or possession of a false or unauthorized military or official pass, permit, discharge certificate, or identification card.

(a) That the accused wrongfully used or possessed a certain military or official pass, permit, discharge certificate, or identification card;

(b) That the pass, permit, discharge certificate, or identification card was false or unauthorized.

(c) That the accused then knew that the pass, permit, discharge certificate, or identification card was false or unauthorized; and

(d) That, under the circumstances, the conduct of the accused was to the prejudice of the good order and discipline in the armed forces or was a nature to bring discredit upon the armed forces.

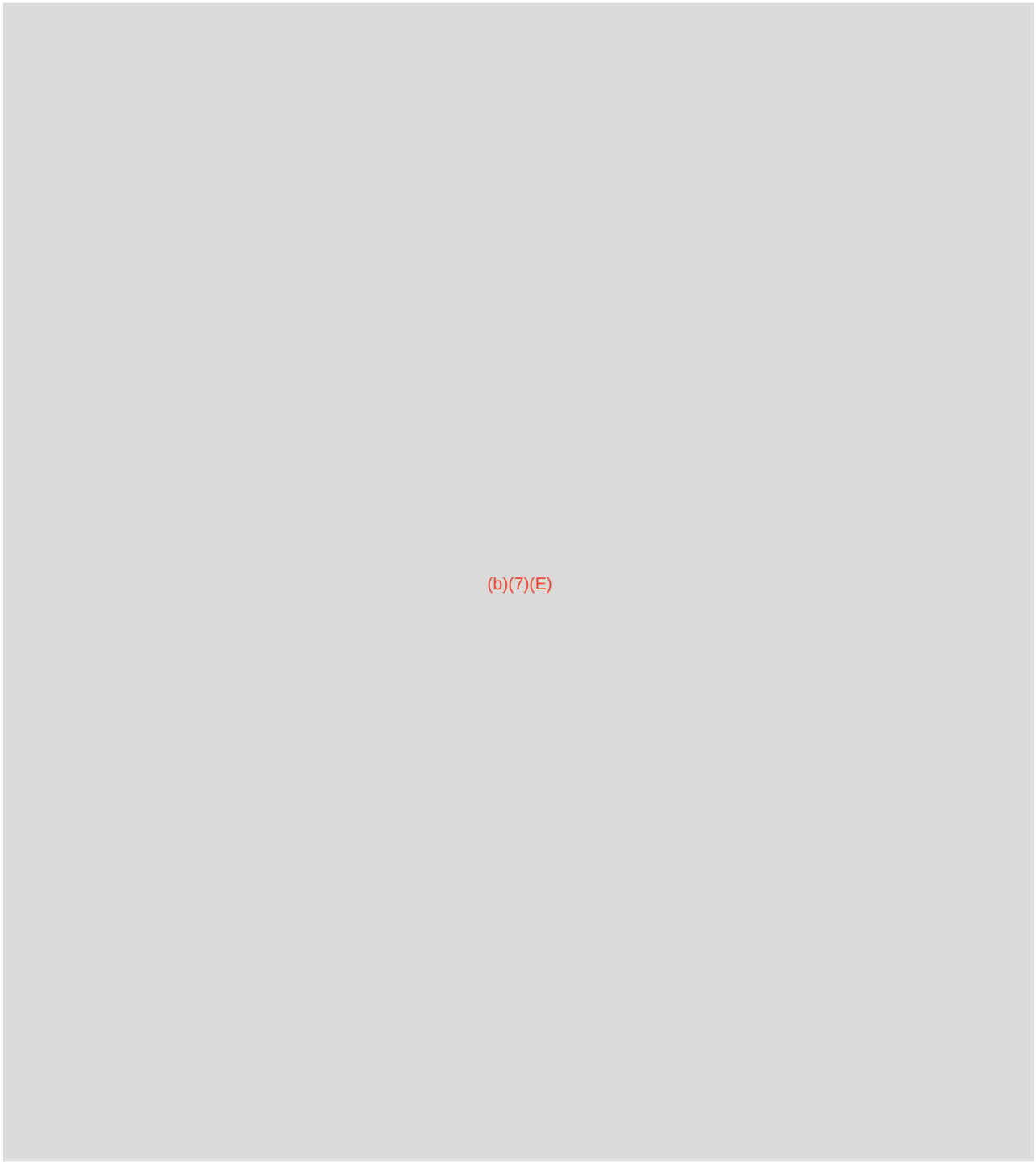
c. Article 134 – General Article (Public Record: Altering, Concealing, Removing, Mutilating, Obliterating, or Destroying).

(1) Public Records. This refers to any records, reports, statements, or data compilations, in any form, of public offices or agencies, setting forth the activities of the office or agency. This also includes matters observed pursuant to duty imposed by law as to which matters there was a duty to report. This includes classified matters.

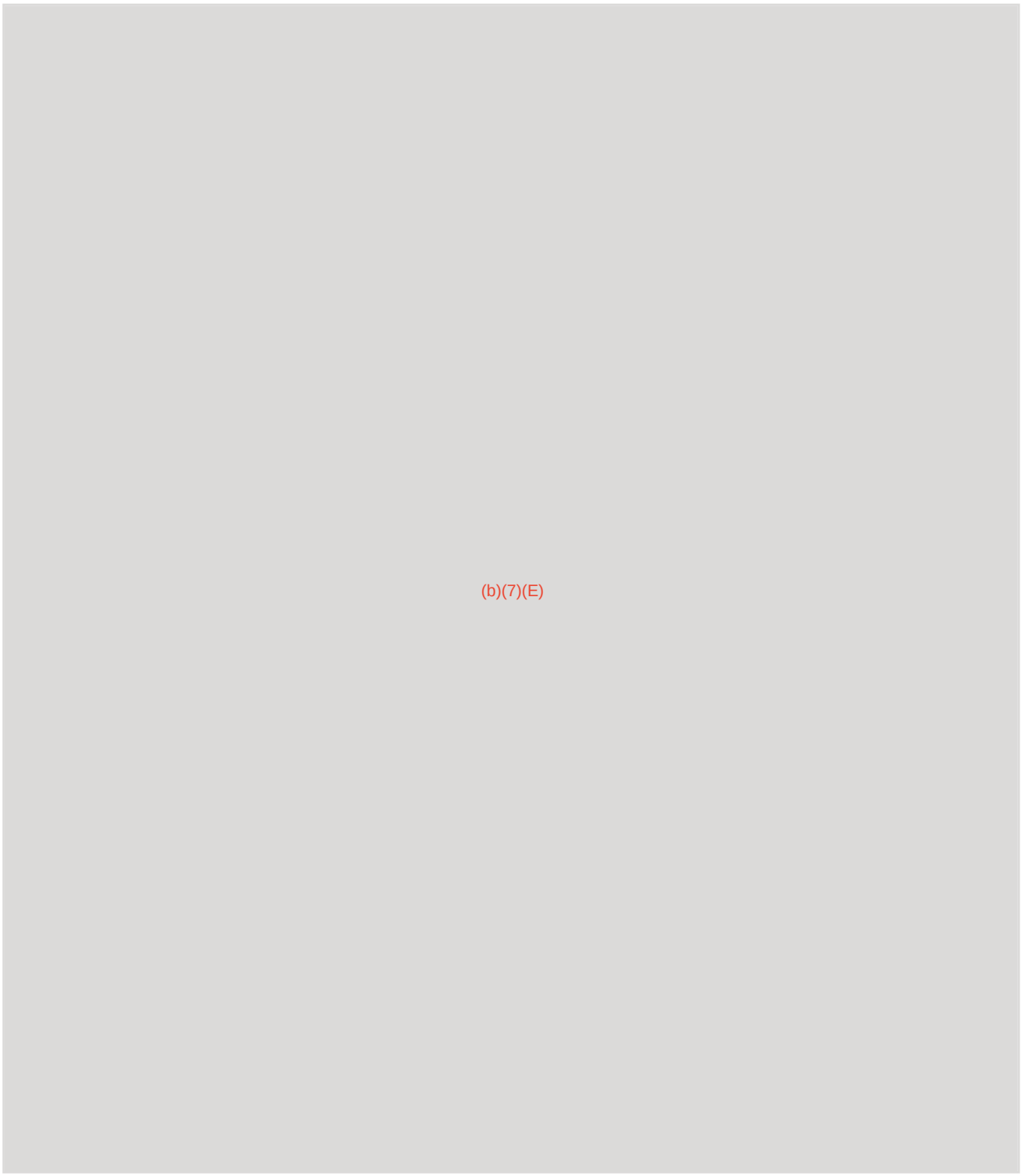
28-4.5. Paper Currency – General. Nations attempt to protect their currency against counterfeiting to insure economic stability and well-being. The United States accomplishes this through vigorous enforcement of the laws that prohibit counterfeiting, and by means of building into the currency certain design and production safeguards. Special agents should be familiar with these safeguards

in order to recognize a counterfeit bill and the pitfalls to which counterfeiters are subject. One of the best ways to recognize counterfeit notes is to compare it with a genuine bill of the same denomination and series. Good currency is made to exact standards by a high quality printing process. Rubbing a bill will not prove whether it is genuine or counterfeit since ink will rub off either type of note.

a. Characteristics of U.S. Currency.



Pages 799 through 802 redacted for the following reasons:
- -
(b)(7)(E)



28-5. POSTAL (6L)

28-5.1. Postal Violations – General. Investigated under case subcategory 6L. This subcategory is used for material pertaining to postal violations, including such matters as loss, theft, rifling, wrongful delivery, delay, or damage of mail in military mail facilities or other places under the

jurisdiction of DoD. Also included would be the theft of stamps, and the theft, alteration, and forgery of postal money orders.

28-5.2. Jurisdiction. The investigation of postal violations is the primary concern of the U.S. Postal Inspection Service (USPIS). However, NCIS personnel are frequently involved in investigating violations of postal regulations when conducting preliminary inquiries to establish that a crime has in fact been committed in conjunction with U.S. Postal Inspectors or in conducting complete investigations in areas where U.S. Postal Inspectors are not available. The USPIS receives its jurisdictional authority from Title 18, U.S. Code, while the authority for NCIS to investigate postal matters lies within the NCIS charter (SECNAVINST 5430.107).

a. Postal inspectors are the fact-finding and investigative agents of the USPIS. Possessing statutory power of arrest, they apprehend violators of the law and work closely with U.S. Attorneys in prosecuting cases in court. Their work also entails the audit of postal operations, the investigation of accidents, and a wide variety of other service and audit matters within the USPS.

b. Under current agreement between the U.S. Postal Service (USPS) and the Military Postal Service Agency (MPSA), the DoD is responsible for policies and regulations concerning the privacy and security of overseas Military Post Offices (MPO). For the purposes of this agreement, overseas is defined as any place outside the United States where the USPS does not operate a civilian post office. This includes those instances when a Naval vessel is operating off shore beyond the 3-mile limit of the United States. Complete instructions relating to this matter can be found in DoD Postal Manual, (DoD 4525.6-M), Chapter 10. Special agents should liaise with both MPO personnel, Staff Judge Advocate (SJA) and USPIS personnel relative to this subject in order to make full use of its benefits. Additionally, the USPS frequently has representatives at U.S. Embassies around the world.

28-5.3. Legal – U.S. Code.

a. Mail Fraud Statute. The Mail Fraud Statute (Title 18 USC Section 1341) is the oldest consumer protection law in the United States, and is one of the most effective prosecutorial tools in fighting white collar and organized crime. It defines fraud as a scheme or artifice which uses the U.S. Mail to obtain money or property by means of false or fraudulent representations. Mail fraud is a criminal scheme where the postal system is used to obtain money or anything of value from a victim by offering a product, service, or investment opportunity that does not live up to its claims. Some of the prevalent schemes include credit card frauds; insurance, banking, inheritance fraud; land and advance-fee selling swindles; franchise schemes; charity schemes; promotions of fake health cures, chain letters, and lotteries. To obtain a mail fraud conviction, a prosecutor must prove:

(1) The facts surrounding the offer were intentionally misrepresented; and

(2) The U.S. Mail (to include military postal service) was relied on to carry out the scheme.

28-5.4. Legal – UCMJ.

a. Article 134 – General Article (Mail: Taking, Opening, Secreting, Destroying, Or Stealing

(1) Mail Matter. This refers to any material or matter deposited in a postal system of any government or any authorized depository thereof or in official mail channels of the U.S. or in any agency thereof, including the armed forces.

(a) The value of the mail matter is not relevant to this crime.

(2) Taking:

(a) That the accused took certain mail matter;

(b) That such taking was wrongful;

(c) That the mail matter was taken by the accused before it was delivered to or received by the addressee;

(d) That such taking was with the intent to obstruct the correspondence or pry into the business or secrets of any person or organization; and

(e) That, under the circumstances, the conduct of the accused was to the prejudice of the good order and discipline in the armed forces or was a nature to bring discredit upon the armed forces.

(3) Opening, secreting, destroying, or stealing:

(a) That the accused opened, secreted, destroyed, or stole certain mail matter;

(b) That such opening, secreting, destroying or stealing was wrongful;

(c) That the mail matter was opened, secreted, destroyed, or stolen by the accused before it was delivered or received by the addressee; and

(d) That, under the circumstances, the conduct of the accused was to the prejudice of the good order and discipline in the armed forces or was a nature to bring discredit upon the armed forces.

28-5.5. Investigative Considerations. No standard guidelines can be laid down to follow in the investigation of these types of violations. The complaint in itself will usually furnish initial investigative leads, and additional leads can be developed as suggested, and the collection and preservation of physical evidence, together with laboratory and handwriting analysis, may frequently play an important part. It will also be necessary during the course of the investigation to determine what statute(s) have been violated in order that evidence bearing on each element of the offense may be sought. This can be accomplished by consultation with postal officers and appropriate legal personnel.

28-5.6. The use of postal service uniforms by NCIS personnel and/or active postal service employees being utilized in undercover operations is prohibited.

28-5.7. Investigative Requests for Records of Postal Money Orders. All investigative requests for the retrieval of records pertaining to postal money orders will be made directly to the U.S. Postal Inspection Service. When requesting information pertaining to postal money orders, the request must be typed on official letterhead and addressed to: U.S. Postal Inspection Service Intelligence Group, National Money Order Coordinator, 475 L'Enfant Plaza SW, Room 3140, Washington, DC 20260-3140. The request must include the reason for the request. The request can be mailed, faxed to (202) 268-4563 or emailed to intelligence@uspis.gov. These records will be retained in the case file and destroyed when appropriate in accordance with current NCIS case destruction procedures.

28-5.8. Search and Seizure of Mail from an MPO. DoD Publication 4525.6-M, Chapter 10, sets forth the procedures for conducting search warrants or command authorized searches at a MPO. In accordance with this regulation, the following conditions must be met for conducting search warrants or search authorizations at a MPO:

a. A search warrant duly issued in accordance with Rule 41 of the Federal Rules of Criminal Procedures will be honored by the MPO.

b. The search authorization must be executed by either a military judge or magistrate authorized by service regulations to issue search authorizations or a Commanding Officer authorized to convene a special court-martial and authorized by the Manual for Courts-Martial (MCM) to issue search authorizations for the particular individual or location. As with any Command Authorized Search, case agents are encouraged to work with the Command Staff Judge Advocate to insure the person that is being petitioned for the search authorization is indeed qualified to execute the search authorization.

c. The search authorization must be executed by a person(s) authorized to conduct the search.

d. The search authorization must be done in the presence of military postal clerk/officer.

e. A copy of the search authorization and an inventory of all items seized must be left with the MPO. The inventory must be made out in the presence of a military postal clerk/officer and, if applicable, should include Registered Mail, Certified Mail, or Insured Mail numbers of any items seized.

f. If the suspected item or items are not found during the search, a letter detailing the circumstances of the search and a copy of the search authorization are to be placed in the letter or package which will be resealed and returned to the MPO for delivery.

28-5.9. DoD Publication 4525.6-M allows for MPO personnel to search mail under several circumstances. While these searches do not fall within the NCIS mission, contraband found during these searches may be seized as evidence. The MPO must treat all other items as personal mail and proceed with the delivery of those items.

a. A letter or package may be searched if a mail clerk/officer reasonably suspects it to pose an immediate danger to life and limb, or an immediate and substantial danger to property. The detention of this item is only authorized to identify and eliminate the threat. This can be accomplished without a search warrant or authorization.

b. In the case of mail not sealed against inspection, the military postal clerk or postal officer may take actions deemed appropriate to determine if the contents of the letter or package are authorized to be mailed under existing USPS guidelines.

c. In some circumstances, MPO personnel may be authorized to open all mail in accordance with local command requirements. This is not an authorization to open individual items.

28-5.10. Mail may be detained for investigative purposes by a military postal clerk/officer when:

a. Acting upon reasonable suspicion, for a brief period of time not to exceed 72 hours, so that military officials acting diligently and without avoidable delay, may assemble evidence sufficient to satisfy the probable cause requirements for search procedures.

b. A military postal clerk or postal officer is acting with the express consent of the addressee or sender.

28-6. CUSTOMS (6M)

28-6.1. The case category Customs (6M) is used for material pertaining to violations of the customs laws and regulations of the United States and foreign governments. Customs is the authority or agency in a country responsible for collecting customs duties and for controlling the flow of animals and goods (including personal effects and hazardous items) in and out of a country. Depending on legislation and regulations, the import or export of some goods may be restricted or forbidden, and the customs agency enforces these rules. In the U.S., the Bureau of Immigration and Customs Enforcement (BICE) and the U.S. Coast Guard (USCG), under the Department of Homeland Security (DHS), are primarily responsible for the investigation of customs violations.

a. Smuggling investigations will be worked under the Customs (6M) case category. Smuggling is the unlawful transport of goods, generally across borders (interstate or internationally) for the purposes of avoiding taxes or customs fees, or in order to transport goods into a location where they are prohibited. Smuggling can involve legitimate goods (e.g., food, medical supplies, etc), illegal goods (e.g., narcotics) or controlled goods (e.g., alcohol, weapons, etc). NCIS investigations involving smuggling could potentially relate to case categories Blackmarketing (6C), Postal (6L) or Special Inquiry (6X), such as war profiteering.

28-6.2. Definition.

a. War Profiteering. Any person or organization that improperly profits from war or conflict by selling weapons and/or other goods to parties at war or in a conflict zone.

28-6.3. Jurisdiction – Customs Matters. Investigative jurisdiction in violations of United States customs regulations is vested in the DHS, mainly between the BICE and the USCG. U.S. Navy Regulations (article 1150) and other U.S. Navy Instructions, prescribe the conditions under which alcoholic beverages (liquor) may be transported on board U.S. Naval ships and aircraft. Violations of this article by personnel on board ships or aircraft returning from overseas will usually involve violation of customs laws and regulations as well. NCIS assistance is often requested to identify the senders/receivers of contraband that has been confiscated by customs.

28-6.4. Legal Considerations. This section discusses possible UCMJ violations that may be used in investigating customs matters. Consult with the proper legal authority in the jurisdiction of the investigation for additional discussion of legal considerations.

a. Article 103 – Captured or Abandoned Property. Refer to section 28-3.2 for a detailed discussion of the elements for UCMJ Article 103.

b. Article 108 – Military Property of the US (Sale, Loss, Damage, Destruction, or Wrongful Disposition). See section 28-3.2 for a detailed discussion of the elements for UCMJ Article 108.

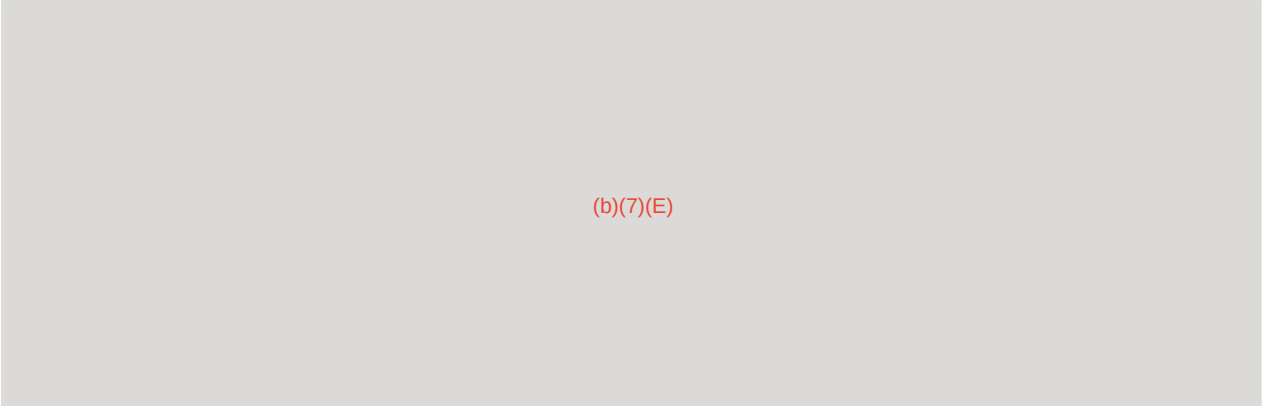
c. Article 134 – General Article (Stolen Property: Knowingly Receiving, Buying, or Concealing). See NCIS-3, Chapter 27 (Larceny) for further explanation of this crime. See section 28-3.2 for a detailed discussion of the elements for UCMJ Article 134.

d. Article 134 – General Article (Mail: Taking, Opening, Secreting, Destroying, or Stealing). See section 28-5.4 for a detailed discussion of the elements for UCMJ Article 134.

e. Article 92 – Failure to Obey an Order or Regulation. This article of the UCMJ is in relation to violating Navy Regulations or instructions prohibiting such acts.

28-6.5. Customs Violations Investigations. Investigative procedures in customs violations cases will be dictated by the circumstances. The exact nature of the violation should be determined as nearly as possible. Usually it will involve smuggling in some form; for example, failing to declare an article being imported, submitting a false declaration, attempting to evade customs inspection altogether, and so forth. If prosecution by court-martial could result, the charge will most likely be made under UCMJ Article 134 (General Article), citing in the specification the verbatim language of the Federal statue violated. Investigation thus should be directed to acquiring evidence on each element of that statute to support successful prosecution. Case agents investigating customs violations should keep the following in mind:

(b)(7)(E)



28-7. SPECIAL INQUIRY (6X)

28-7.1. This subcategory is used for investigations pertaining to matters of unique interest to the Navy requiring the application of special investigating techniques or handling and for situations which, because of infrequent occurrence, or for other reasons, is not specifically covered by any of the above subcategories. Special Inquiry (6X) type investigations can include war profiteering, racketeering, and fencing.

a. "Blank" Military Identification Cards or Vehicle Decals. Stolen "blank" military or civilian identification cards (e.g., Common Access Cards (CAC)) and vehicle decals (i.e., "pass and ID" decals) may be a significant security issue or potentially used to commit other offenses. The theft of "blank" identification cards or decals should be investigated under the Special Inquiry (6X) subcategory. NCISHQ Code 21 (Combating Terrorism Directorate (CbT)) should be included as an INFO addee to the ROI. Refer to NCIS-3, Chapter 38 for guidance on Suspicious Incident (5Y) and Terrorism (5T) investigations. The initiation of an investigation regarding theft of "blank" ID cards or decals will be left to the discretion of the cognizant NCIS office when a minimal number of cards or decals are involved. However, it is generally not the policy of NCIS to investigate individual missing or stolen military identification, vehicle decals or passes; unless it is an indication of a larger criminal or force protection matter. "Blank" military identification and decals that have been altered with fraudulent or legitimate personal information should be investigated as counterfeiting (6G).

b. War Profiteering. War profiteering is any person or organization that improperly profits from war or conflict by selling weapons and/or other goods to parties at war or in the conflict zone. On a larger scale this may involve a procurement fraud or economic crimes if corporations, contracts or large sums of money are involved (see NCIS-6 manual on economic crimes). On a smaller scale, this may involve military members, contractors, or government employees attempting to sell or transport "war trophies," contraband, or illegally seized items in the combat zone. In such instances this may be potentially investigated as Blackmarketing (6C), Customs (6M) violations, or a Special Inquiry (6X).

28-7.2. Legal Considerations. This section discusses possible UCMJ violations that may be used in special inquiry investigations. Consult with the proper legal authority in the jurisdiction of the investigation for additional discussion of legal considerations.

a. Article 103 – Captured or Abandoned Property. Refer to section 28-3.2 for a detailed discussion of the elements for UCMJ Article 103.

b. Article 108 – Military Property of the US (Sale, Loss, Damage, Destruction, or Wrongful Disposition). See section 28-3.2 for a detailed discussion of the elements for UCMJ Article 108.

c. Article 134 – General Article (Stolen Property: Knowingly Receiving, Buying, or Concealing). See NCIS-3, Chapter 27 (Larceny) for further explanation of this crime. See section 28-3.2 for a detailed discussion of the elements for UCMJ Article 134.

d. Article 134 – General Article (False or Unauthorized Pass Offenses). See section 28-4.4 for a detailed discussion of the elements for UCMJ Article 134.

e. Article 134 – General Article (Mail: Taking, Opening, Secreting, Destroying, or Stealing). See section 28-5.4 for a detailed discussion of the elements for UCMJ Article 134.

f. Article 134 – General Article (Public Record: Altering, Concealing, Removing, Mutilating, Obliterating, or Destroying). See section 28-4.4 for a detailed discussion of UCMJ Article 134.

g. Article 92 – Failure to Obey an Order or Regulation. This article of the UCMJ is in relation to violating Navy Regulations or instructions prohibiting such acts.

CHAPTER 29
TITLE: ASSAULT (CATEGORY 7G AND 7V)
POC: CODE 23A
DATE: AUG 08

29-1. DISCUSSION

29-1.1. General. The following chapter discusses general information pertinent to assaults, the definitive distinctions between aggravated and simple assault (case category 7G), and the use of assaults to commit other crimes, with the exception of sexual assault, but including family violence and domestic assaults (case category 7V).

29-1.2. Definitions

a. Assault. An attempt or offer to do bodily harm to another with unlawful force or violence, whether or not the attempt or offer is consummated.

b. Domestic Assault. An assault directed toward a person of the opposite sex who is: (a) a current or former spouse; (b) a person who shares a child in common with the assailant; or (c) a current or former intimate partner with whom the assailant shares or has shared a common domicile.

c. Battery. An assault in which the attempt or offer to do bodily harm is completed by the infliction of that harm.

d. Aggravated Assault. An assault with or without a dangerous weapon or other means or force likely to produce death or grievous bodily harm.

29-1.3. Criminal Law/Jurisdiction

a. Uniform Code of Military Justice (UCMJ). Crimes of this category are potentially violations of UCMJ:

Article 90 (Assaulting or Willfully Disobeying a Superior Commissioned Officer)
Article 92 (Failure to Obey an Order or Regulation)
Article 128 (Assault)

Article 134 (General Article - Assault with Intent to Commit Murder, Voluntary Manslaughter, Rape, Robbery, Sodomy, Arson, Burglary, or Housebreaking)
Article 134 (General Article – Obstructing Justice)
Article 134 (General Article – Reckless Endangerment)

b. Federal Laws/United States Code (USC). Crimes of this category are potentially violations of Title 18 USC:

Chapter 7 (Assault)
Chapter 90A (Protection of Unborn Children)
Chapter 110A (Domestic Violence and Stalking)

c. State Criminal Law. Depending on jurisdiction and/or victim/suspect of crimes of this category (i.e., non-military personnel or government property), appropriate state penal code may apply. States and local criminal laws relating to assaults may differ in definitions and elements of the offenses covered in this chapter.

29-2. POLICY AND GUIDANCE

29-2.1. Naval Criminal Investigative Service (NCIS) Authority. NCIS authority and jurisdiction to investigate these categories of offenses are derived from SECNAVINST 5430.107. DoD Instruction 5525.07 (18JUN07) implements the Memorandum of Understanding (MOU) between the Department of Justice and the Department of Defense (DoD) criminal investigative organizations. This MOU provides policy and guidance for criminal investigations when both departments have jurisdiction. See NCIS-3, Chapter 1 (Authority, Jurisdiction, Scope) for further explanation.

29-2.2. NCIS Responsibility. Per SECNAVINST 5430.107, NCIS has the primary responsibility for liaison between law enforcement entities and the Department of the Navy (DON) elements for the purposes of investigations.

a. If NCIS investigates any of the crimes described in this chapter and when logical to the investigation, a detailed crime scene examination should occur, to include photographs, diagrams/sketches, evidence collection, and taking any victim and/or witness statements. Attempts should be made to employ forensic techniques as appropriate.

b. If a NCIS investigation is initiated on any of the crimes described in this chapter, liaison with the local security force and/or police departments of adjacent communities and/or federal law enforcement entities should occur. Any police reports or incident reports made by other law enforcement entities should be requested as part of the investigation.

c. The investigating agent(s) should take written statements from the victim(s), pertinent witnesses, and from the interrogation of suspects.

29-2.3. The crimes of assault with intent to commit murder and attempted murder should be investigated as an Assault (7G). Should there be a demise of the assaulted victim, the

investigation should be treated as a death investigation (7H).

29-2.4. Domestic Assault Investigations. NCIS investigates domestic assaults (including misdemeanor or simple assaults) under the following circumstances:

a. The assault was committed with a weapon; and/or

b. Serious bodily injury occurred as the result of the assault; and/or

c. Attempted strangulation; and/or

d. The victim is pregnant or recently gave birth; and/or

e. Prior incidents of violence that appear to be escalating in severity.

29-2.5. Victim and Witness Assistance Program (VWAP). The responding and/or investigating agents will provide VWAP Forms and information to the victim(s) of the assault. The victim shall be provided with information regarding advocate availability, family service center locations, domestic violence hotlines, and ways to obtain civilian support assistance. In addition, a victim's advocate should be notified prior to departure so that contact information may be collected for advocacy files. Witnesses may also be given VWAP forms as deemed appropriate to the circumstances. VWAP advisement will be documented in the investigating agent's Case Activity Report (CAR) and in an Investigative Action (IA).

29-2.6. Threat Management Unit (TMU). The NCIS TMU may be requested by the investigating agent in investigations involving domestic violence or situations of escalating violence. For a full explanation of the TMU, refer to NCIS-3, Chapter 33 (Crimes Against Persons – Other). The TMU can provide agents with criminal and behavioral analysis and risk assessments for the potential for future violence. The level of coordination in these cases varies with each investigation.

a. To request TMU assistance, contact the local TMU Field Office representative or the NCISHQ Code 23B TMU desk officer. If appropriate, a threat assessment will be provided to the field and is to be utilized by the case agent as "case notes." The assessment will not be attached to any external reports without TMU approval, but may be used to verbally brief commands and other concerned parties. Agents in the field are not advised to send a request via a ROI (ACTION).

29-2.7. Investigation of Simple Assaults. Simple assault involves nothing more than an attempt to harm, an offer to harm, or actual physical contact, without weapons, which cannot be categorized as aggravated. Simple assaults are misdemeanors and should normally be investigated by base investigators, such as CID, MAA Force, or Base Security.

a. Incidents that result in injuries (including minor) to a victim who is pregnant or recently gave birth, any attempted strangulation, or when the number of domestic altercations clearly indicate a pattern of escalating violence in severity and occurrence, then the criteria is met for a

Domestic Assault (7V) investigation. NCIS may provide limited investigative assistance to CID, Family Advocacy Program (FAP), or local law enforcement upon request.

b. It is the responsibility of NCIS to ensure all non-NCIS controlled domestic violence investigations occurring off base are documented in the Defense Central Index of Investigations (DCII) system in a timely manner. At a minimum, the following information should be included: NI title block information (obtained by reviewing the police report); information about how injury was inflicted; arrest information to include appropriate statutes; National Crime Information Center (NCIC), criminal/Family Advocacy Program (FAP) checks, local criminal history checks; and final court disposition information. When noting that criminal history checks were conducted, it is imperative the NCIC criminal history is NOT detailed if the report is disseminated outside of law enforcement channels (i.e., Command or FAP). It should merely state, "Criminal history checks were conducted." If the information can be obtained and reported in ten (10) business days, a ROI (CLOSED) may be used to document the details, noting under the ACTION caption that it is an "Only Report." Otherwise, a ROI (OPEN) should be used to initiate case activity. If the disposition is not known at the time of closure, a ROI (SUPP) must be submitted once the disposition is known.

c. Hate crimes (e.g., racial incidents) are of interest to NCIS only to the degree that they may involve major criminal offenses. See NCIS-3, Chapter 33 (Crimes Against Persons – Other) for further explanation of hate crimes.

29-3. ELEMENTS OF THE CRIME

29-3.1. Essential Elements of Assault. The essential elements of assault under Articles 90, 91, 128, and 134 of the UCMJ and the applicable statutes in Title 18, Sections 111-115 of the USC require that:

a. The accused was a person subject to Federal jurisdiction or the UCMJ at the time of the offense, and

b. The assailant attempted or offered to do bodily harm to another person using unlawful force or violence.

29-3.2. Assault Statute in the UCMJ. Under the UCMJ, the crime of assault is divided into general Assault and Aggravated Assault. The statute relating to assault under the UCMJ is as follows:

a. Assault (General). Any person subject to the UCMJ who attempts or offers with unlawful force or violence to do bodily harm to another person, whether or not the attempt or offer is consummated has committed an assault.

b. Aggravated Assault. Any person subject to the UCMJ who:

(1) Commits an assault with a dangerous weapon or other means or force likely to produce death or grievous bodily harm; or

(2) Commits an assault and intentionally inflicts grievous bodily harm with or without a weapon.

29-3.3. Elements of Assault (General) and of Battery. The elements of a general Assault under the UCMJ are as follows:

a. Simple Assault.

(1) That the accused attempted or offered to do bodily harm to a certain person; and

(2) That the attempt or offer was done with unlawful force or violence.

b. Assault Consummated by a Battery.

(1) That the accused did bodily harm to a certain person; and

(2) That the bodily harm was done with unlawful force or violence.

29-3.4. Legal Discussion – Simple Assaults and Batteries. Both simple assaults and related battery are not considered felony level violations; however, simple assaults where the victim is of a certain status or particular situations may result in potentially felony level offenses. These assaults with increased punishment (i.e., felony level) based on victim's status or particular situation are as follows:

a. Assaults upon a commissioned officer or warrant officer of the armed forces of the U.S. or of a friendly foreign power, not in the execution of office.

b. Assaults committed with an unloaded firearm.

c. Assaults upon a sentinel or lookout in the execution of duty.

d. Assaults upon any person who, in the execution of office, is performing security police, military police, shore patrol, master at arms, or other military or civilian law enforcement duties.

e. Assault consummated by a battery upon a child under 16 years.

29-3.5. Elements of Aggravated Assault. The elements of an aggravated assault under the UCMJ are as follows:

a. Assault with a Dangerous Weapon or Other Means of Force Likely to Produce Death or Grievous Bodily Harm.

(1) That the accused attempted to do, offered to do, or did bodily harm to a certain person;

(2) That the accused did so with a certain weapon, means, or force;

(3) That the attempt, offer, or bodily harm was done with unlawful force or violence; and

(4) That the weapon, means, or force was used in a manner likely to produce death or grievous bodily harm.

b. Assault in Which Grievous Bodily Harm is Intentionally Inflicted.

(1) That the accused assaulted a certain person;

(2) That grievous bodily harm was thereby inflicted upon such person;

(3) That the grievous bodily harm was done with unlawful force or violence; and

(4) That the accused, at the time, had the specific intent to inflict grievous bodily harm.

NOTE: The following are additional elements (i.e., making the offense further "aggravated") depending on the circumstances of the incident:

(1) That the weapon was a loaded firearm;

(2) That the person was a child under the age of 16 years.

29-3.6. Legal Discussion – Assaults. An "assault" is an attempt or offer with unlawful force or violence to do bodily harm to another, whether or not the attempt or offer was completed. It must be done without legal justification or excuse and without lawful consent of the victim.

a. Offers and Attempts. The "offer" is an unlawful demonstration of violence. An offer to do bodily harm is distinguished from an attempt in that an offer implies that the victim is instilled with reasonable fear that bodily harm will be immediately inflicted upon the victim. A specific intent to inflict the bodily harm is not required for an "offer." An "attempt" requires specific intent to inflict the bodily harm and an overt act. The overt act must amount to more than mere preparation and apparently tends to go toward the inflicting of bodily harm. An attempt may be committed even though the victim had no knowledge of the incident at the time.

(1) Example of an Offer. An assailant knowingly points an unloaded pistol at the victim; however, the assailant is not necessarily considering to do bodily harm. The victim's reasonable fear of bodily injury from the attack may be considered an offer.

(2) Example of an Attempt. An assailant throws a punch at the victim, intending to hit him but missing. The assailant has committed an attempt, whether or not the victim was aware of the attempt.

c. If the circumstances to the person menaced clearly negate the intent to cause bodily harm, an assault has not occurred. For example, a case in which an accused assailant raises a club, shakes it at a complainant within striking distance while stating, "I would knock you down if you weren't such an old man" does not constitute assault. An offer to instantly inflict bodily injury upon another in

compliance with an unlawful demand, however, would be considered assault. For example, an assailant stating "I will shoot you if you don't give me your watch" to a victim has committed an assault.

d. Battery. An assault in which the attempt or offer to do bodily harm is consummated by the infliction of such harm is called a battery. Battery may be defined as an unlawful, intentional, or illicitly negligent application of force to another personally by hand or foot or head-butt, or the like, and through the use of an object, either directly or indirectly. For example, the use of a dog to attack, the use of a gun to shoot, the facilitating of the ingestion of poison, and striking with an automobile upon another person are all considered incidents of battery. Proof of an incident of battery generally supports evidence of the occurrence of assault.

e. Unlawful Force or Violence. An act of violence must be deemed unlawful to constitute assault. The lawful consent of the person affected and/or legal justification or excuse must not be evident. Persons cannot generally consent to violent activity that creates a breach of the peace. Therefore, under the law, a mutual affray might be an assault by both persons. Additionally, a victim cannot consent to an act done with the specific intent to inflict grievous bodily harm. For example, an uninfected female service member's informed consent to unprotected sexual intercourse with an HIV-positive accused is not a defense to aggravated assault.

(1) Proof that a battery, as well as an attempt or offer to do bodily harm, to another by an accused must be shown to have occurred with unlawful force or violence.

(2) The use of threatening words alone does not necessarily provide grounds for assault. Threatening words accompanied by a menacing act or gesture may be evidence of assault, since a combination may demonstrate an act of violence.

f. Bodily Harm. An object is considered a dangerous weapon when used in a manner that is likely to produce death or grievous bodily harm. Grievous bodily harm does not include minor injuries, such as a black eye or a bloody nose, but does include fractured or dislocated bones, deep cuts, torn members of the body, serious damage to internal organs and other serious bodily injuries, and includes instances when the natural and probable consequence of a particular use of any means or force is likely to produce that result.

(1) Actual death or grievous bodily harm does not necessarily have to result to be considered an offense of aggravated assault with a dangerous weapon, or other means of force. Other means of force refers to any means or instrument(s) not normally considered a weapon.

(2) When grievous bodily harm has been inflicted by means of intentionally using force in a manner likely to achieve that result, it may be inferred that grievous bodily harm was intended. For example, intentionally knocking a person from a high grandstand so that the resulting fall breaks his leg constitutes an aggravated assault in which grievous bodily harm is intentionally inflicted.

29-3.7. Legal Discussion – Domestic Assault. Domestic assaults are distinguished by the relationship between the assailant and the victim. Domestic assault involves an assault directed against another person who is:

a. A current or former spouse;

b. A person with whom the assailant shares a child in common with the victim;

c. A current or former sexually intimate relationship; or

d. A family member living in the same domicile as a DON affiliated member.

(1) Domestic assault also may implicate violations of a lawful order issued for the protection of an adult.

(2) Domestic violence is a complex pattern of behavior involving the increasingly frequent and escalating physical, psychological and/or other abusive behaviors used to control another person. Violent relationships rarely start as abusive, as affection and physical intimacy usually precede incidents of abuse. As a result, it is often difficult for the victims to leave abusers, as abusive actions may be temporarily replaced with loving and nurturing behavior. It is commonly recognized that the most dangerous time for a domestic violence victim is during attempts to end the relationship with the abuser.

29-3.8. Elements of Assault with Intent to Commit Murder, Voluntary Manslaughter, et al. The elements of this general article (Article 134) under the UCMJ are as follows:

a. That the accused assaulted a certain person;

b. That, at the time of the assault, the accused intended to kill (as in case of murder or voluntary manslaughter) or intended to commit rape, robbery, sodomy, arson, burglary, or housebreaking; and

c. That, under the circumstances, the conduct of the accused was prejudice of good order and discipline in the armed forces or was of a nature to bring discredit upon the armed forces.

29-3.9. Legal Discussion – Assault with Intent to Commit Murder, Voluntary Manslaughter, et al.

a. An assault with intent to commit any of the mentioned offenses (in this UCMJ article) is not necessarily the equivalent of an attempt to commit the intended offense, for an assault can be committed with intent to commit an offense without achieving that proximity to consummation of an intended offense which is essential to an attempt.

b. Assault with intent to commit murder is assault with specific intent to kill. Actual infliction of injury is not necessary. When the intent to kill exists, the fact that for some unknown reason the actual consummation of the murder by the means employed is impossible is not a defense if the means are apparently adapted to the end in view.

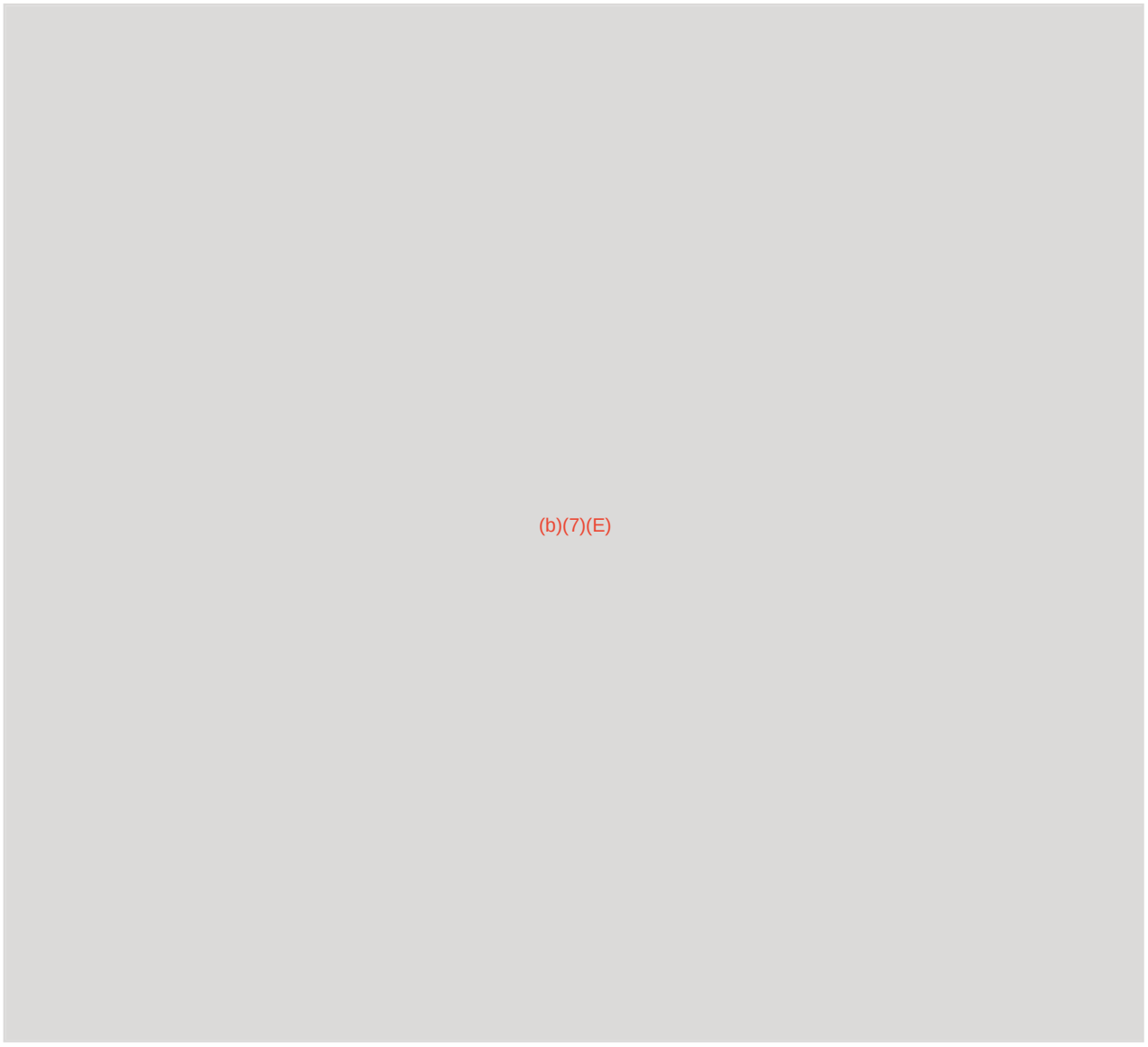
c. Assault to commit voluntary manslaughter is an assault committed with a specific intent to kill under such circumstances that, if death resulted therefrom, the offense of voluntary manslaughter would have been committed. There can be no assault with intent to commit involuntary

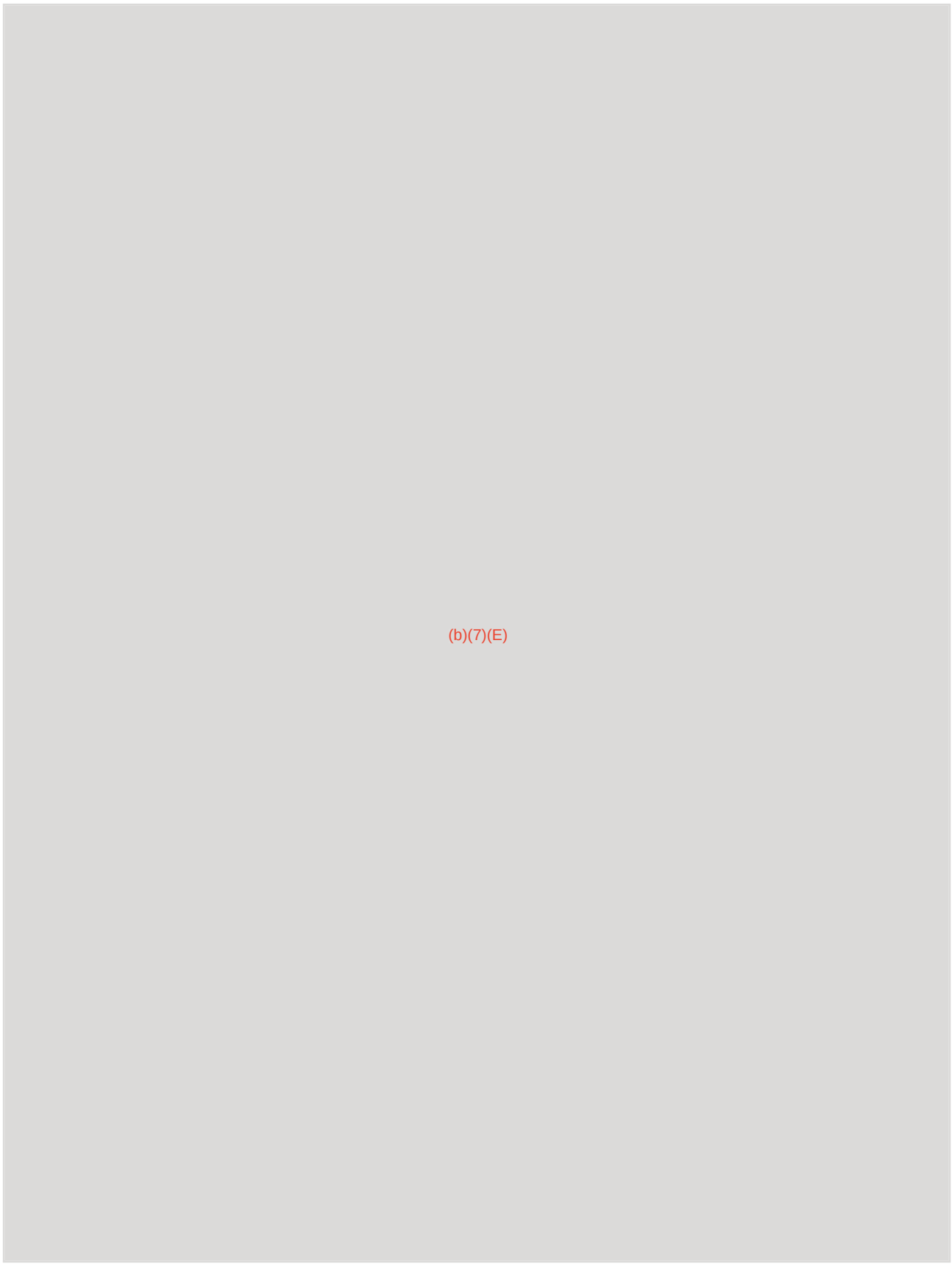
manslaughter, for it is not a crime capable of being intentionally committed.

29-3.10. Legal Discussion – Obstructing Justice. This offense may be based on conduct that occurred before or after preferral of charges. Examples of obstruction of justice include wrongfully influencing, intimidating, impeding, or injuring a witness by means (for purposes of discussion of assault) of intimidation, force, or threat of force in order to delay or prevent communication of information relating to a violation of any criminal statute of the United States.

29-3.11. Legal Discussion – Reckless Endangerment. This offense is intended to prohibit and deter reckless or wanton conduct that wrongfully creates a substantial risk of death or grievous bodily harm to others. Conduct is "wrongful" when it is without legal justification or excuse. It is not necessary that death or grievous bodily harm be actually inflicted to prove reckless endangerment.

29-4. INVESTIGATIVE CONSIDERATIONS




(b)(7)(E)

Pages 821 through 837 redacted for the following reasons:
- -
(b)(7)(E)

CHAPTER 30
TITLE: DEATH INVESTIGATIONS
POC: CODE 23A
DATE: APR 08

APPENDICES

(6) PSYCHOLOGICAL AUTOPSY, PSYCHOLOGICAL REVIEW – INVESTIGATIVE QUESTIONS IN EQUIVOCAL DEATH CASES
(7) DEATH REVIEW BOARD/PANEL CHECKLIST
(8) MEMORANDUM OF AGREEMENT (MOA) BETWEEN THE NAVAL SAFETY CENTER (NSC) AND NAVAL CRIMINAL INVESTIGATIVE SERVICE (NCIS)

30-1. GENERAL

30-1.1. This chapter provides policy and guidance for Naval Criminal Investigative Service (NCIS) personnel engaged in the investigation of deaths that occur in medically unattended circumstances. Successful completion of a death investigation requires the coordination of the investigative skills of agents, forensic consultants, pathologists, and scientists. NCIS shall initiate an investigation of all medically unattended deaths to assist in determining whether death resulted from homicide, suicide, natural causes, or accidental means.

30-1.2. All NCIS investigations regarding medically unattended deaths are conducted under Case Category 7H, Death. A number of criminal offenses are investigated under this category, including: murder, voluntary and involuntary manslaughter, negligent homicide, and conspiracy and/or solicitation to commit murder. Crimes of assault with intent to commit murder and attempted murder will be investigated under Case Category 7G, Assault. However, should there be a death of the assault victim, the case category will be changed to 7H.

30-2. MURDER

30-2.1. Elements of Murder

a. Under the Uniform Code of Military Justice (UCMJ), Article 118, murder is defined as the unlawful killing of a human being. The killing of a human being is unlawful when done without justification or excuse. The determination of whether an unlawful killing constitutes murder, or a lesser offense, depends upon the circumstances under which it occurred. Offenses are considered to be committed at the place of the acts or omissions, although the victim may have died elsewhere. Murder is constituted when death is the result of an injury received as a consequence of an act or omission.

b. Murder is considered premeditated when the thought of taking life was consciously conceived and the act or omission by which it was taken was intentional. Premeditated murder is murder when it is committed after the formation of a specific intent to kill and consideration of the act intended, but the intention to kill does not have to be entertained for a particular or considerable length of time. An individual with a premeditated design attempting or intending to unlawfully kill a certain person, but inadvertently kills another, is still criminally responsible for a premeditated murder. The premeditated design to kill is transferred from the intended victim to the actual victim.

c. A homicide committed in the perpetration or attempted perpetration of the offenses of burglary, sodomy, rape, robbery, or aggravated arson constitutes murder, whether the homicide was intentional, unintentional, or accidental.

d. An unlawful killing without premeditation is murder when committed with the intent to kill or to inflict great bodily harm. Intent need not be directed toward the person killed, nor exist for any particular time before commission of the act; it is sufficient that intent existed at the time of the act or omission (except if death was inflicted in the heat of a sudden passion caused by adequate provocation). Great bodily harm (also known as "grievous bodily harm") refers to serious injuries such as fractured or dislocated bones, deep cuts, torn members of the body, or serious damage to internal organs. Minor injuries, such as a black eye or bloody nose, are not considered injuries in this category.

e. A homicide committed in the proper performance of a legal duty is justifiable. The duty may be imposed by statute, regulation, or order. For example, killing an enemy combatant in battle is justified. Also, killing to prevent the commission of an offense attempted by force or surprise (e.g., rape or burglary) may constitute justifiable homicide.

f. The general rule is that acts of a subordinate, done in good faith in compliance with his supposed duty or orders, are justifiable. Justification does not exist when acts are manifestly beyond the scope of the superior's authority; or an order is such that a person of sound judgment would understand the act to be illegal. Justification also does not exist if during the discharge of one's duties to prevent an escape or affect an arrest, the subordinate willfully or through negligence commits acts that endanger the lives of innocent parties.

g. A person free from fault has the right to use reasonable force to defend against immediate bodily harm threatened by the unlawful act of another. Self-defense is justified for a killing if the accused's apprehension of death or grievous bodily harm is one that a reasonable, prudent person would have held under the circumstances. Death must have been an unintended or unexpected result of the accused's proper exercise of the right to self-defense. Self-defense may be based on reasonable grounds that killing was necessary to save one's life or the lives of those one might lawfully protect, or to prevent great bodily harm to self or others. Failure to retreat when possible does not deprive the accused of the right to self-defense if the accused was lawfully present. The right to self-defense requires that the individual must not have been the aggressor or have intentionally provoked the altercation. However, if after provocation, one withdraws in good faith and his adversary follows and renews the fight, the adversary may then be considered the aggressor and self-defense may then be justified.

30-2.2. Proof in Murder Cases. The following must be proven to establish murder:

a. The named or described victim is dead;

b. The victim's death resulted from the act or omission of the accused;

c. The killing was unlawful; and

d. The facts and circumstances showed the accused had a premeditated design or intention to kill or inflict great bodily harm; or was engaged in an act inherently dangerous to others, evincing a wanton disregard of human life; or was engaged in the perpetration or attempted perpetration of burglary, sodomy, rape, robbery, or aggravated arson.

30-3. MANSLAUGHTER

30-3.1. Elements of Manslaughter

a. Under the UCMJ, Article 119, voluntary manslaughter is defined as an unlawful killing committed in the heat of sudden passion caused by adequate provocation. The law recognizes that, in the heat of sudden passion caused by provocation, a person may strike a fatal blow beyond one's control. While the law does not excuse the homicide as a result of provocation, it does not consider the act to be murder.

b. Provocation, according to the law, must be deemed adequate to excite uncontrollable passion in the mind of a reasonable person, and the act of killing must be committed under and because of that passion. If sufficient time elapses between the provocation and the killing, allowing the person to "cool down" or regain composure, the act may be considered murder, regardless of the persistence of passion. Provocation must not be sought or induced as an excuse for the killing. Examples of adequate provocation to constitute voluntary manslaughter include: assault and battery inflicting great or grievous bodily harm, unlawful imprisonment, and witnessing of spouse in an adulterous act.

c. Under the UCMJ, Article 119, involuntary manslaughter is an unlawful homicide committed without intent to kill or inflict great bodily harm. It is an unlawful killing by culpable negligence or while perpetrating or attempting to perpetrate an offense other than burglary, sodomy, rape, robbery, or aggravated arson, directly affecting the person. (An offense affecting a particular person is distinguished from an offense affecting society in general; examples include: specific types of assault, battery, false imprisonment, voluntary engagement in an affray, and maiming.) Culpable negligence is a degree of carelessness greater than simple negligence; meaning that it is a negligent act or omission accompanied by a culpable disregard for the foreseeable consequences to others as a result. Examples of culpable negligence acts include: negligently conducting target practice within bullet range of an inhabited house; pointing and pulling the trigger of a pistol in jest, believing there to be a lack of danger but not taking reasonable precautions to make certain; and carelessly leaving poisons or dangerous drugs where they may imperil life.

d. Intentionally engaging in an act inherently dangerous to others without any intent to cause the death of or great bodily harm to any particular person may also constitute murder if the act shows a wanton disregard for human life. Wanton disregard for human life is indifference to the likelihood of death or great bodily harm, or heedlessness of the probable consequences of an act or omission. Examples of such an act include the throwing of a live hand grenade toward another in jest or the flying of an aircraft very low over a crowd to cause scattering.

30-3.2. Proof in Manslaughter Cases. The following must be proven to establish manslaughter:

a. The named or described victim is dead,

b. The death resulted from the act or omission of the accused,

c. The killing was unlawful, and

d. The facts and circumstances show the homicide amounted in law to the degree of manslaughter alleged.

30-4. NEGLIGENT HOMICIDE

30-4.1. Elements of Negligent Homicide. Under the UCMJ, Article 134, negligent homicide is any unlawful homicide that is the result of simple negligence. Intent to kill or injure is not required. Simple negligence is the absence of due care; that is, an act or omission of a person obligated to use due care lacking the degree of care for the safety of others in which a reasonably prudent person would have exercised under the same or similar circumstances. Simple negligence is a lesser degree of carelessness than culpable negligence.

30-4.2. Proof in Negligent Homicide Cases

a. The named or described victim is dead;

b. The death resulted from the act or failure to act of the accused;

c. The killing by the accused was unlawful;

d. The act or failure to act of the accused which caused the death amounted to simple negligence; and

e. That, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces or was of a nature to bring discredit upon the armed forces.

30-5. JURISDICTIONAL ASPECTS

30-5.1. NCIS jurisdiction requires investigative jurisdiction over a suspect(s), victim(s), or place of offense. While NCIS jurisdiction over the place of offense may be immediately established, jurisdiction over suspect(s) and/or victim(s) may not be immediately known. In such cases, NCIS shall conduct a preliminary investigation to establish primary jurisdiction. In those instances where NCIS does not have primary investigative jurisdiction, the investigation will normally be conducted concurrently with the appropriate law enforcement agency having primary investigative jurisdiction, with NCIS serving an appropriate supporting role.

30-5.2. SECNAVINST 5430.107 states that NCIS shall investigate any non-combat death, on or off DON installations, facilities, vessels or aircraft, where the cause of death cannot be medically attributable to disease or natural causes. NCIS will investigate the circumstances until criminal causality can reasonably be excluded. Medically attributable is a term synonymous with "medically attended" death. Since many state codes vary on the definition of medically attended death and many offices have different working definitions, the following definition is NCIS policy:

a. Medically attended death is defined by NCIS as an individual's death while undergoing treatment by a medical officer or physician for a disease or condition that is recognized as a life threatening condition, when the death is determined to have been a logical result of the disease. It is not necessary for the deceased patient to have expired with a physician in direct attendance; to have expired in a hospital; or for the deceased to have seen the physician within a certain period of time prior to the death. It is only necessary for the physician to be able to certify the death was a logical result of a life-threatening disease. For example, a medical officer is treating a service member suffering from terminal cancer and the service member dies in his quarters. The medical officer signs the death certificate attesting the cause of death as cancer and the manner of death as natural. Once determined to be a medically attended death, no further NCIS investigation is required. In a second scenario, a service member treated at a naval hospital for flu-like symptoms is prescribed medication and then sent home for bed rest. On the following morning, the service member is discovered dead and a medical officer cannot certify the cause of death without an autopsy. Typically, without a cause of death, the manner of death cannot be determined. By definition, this situation is not a medically attended death and requires further investigation until criminal causality can reasonably be excluded.

30-5.3. In situations where state codes may conflict with the NCIS definition(s) and the state has a vested interest in a matter, the Special Agent in Charge (SAC) will make the decision regarding what investigative efforts are undertaken, if any.

30-5.4. In the United States, incidents involving the occurrence of medically unattended deaths of service members within the primary jurisdiction of local authorities should be carefully analyzed prior to an investigation commitment by NCIS. Requests by local authorities for investigative assistance in such incidents will be granted within the limits of NCIS investigative jurisdiction and capabilities. Reciprocal cases opened under these conditions should specifically state the assistance requested. If the manner of death is determined to be homicide and the suspect is (or is reasonably believed to be) Department of Defense (DoD) personnel, a joint investigation can be pursued without a specific request for assistance. Cases other than homicide should be specific in scope.

a. NCIS should not attempt to further investigate a death case conducted by competent local authorities unless special and extenuating circumstances exist. Decisions by NCIS to investigate should be briefed to the local authorities, which may also choose to reopen or further pursue the investigation if so desired. Death investigations conducted by local authorities without NCIS assistance will be reported as details and disposition cases in the NCIS Report of Investigation (ROI).

30-5.5. Investigation of a medically unattended death on a base, vessel, or aircraft will be conducted until the SAC determines that the possibility of criminal causality on the part of any living person is not evident. Cases of homicide, suicide, and self-inflicted accidental deaths (including autoerotic) warrant full and complete investigative coverage. (See section 30-14 for guidance regarding homicide, suicide or accidental death, excluding autoerotic death.)

a. The following are two example situations to illustrate an investigation involving a medically unattended death:

(1) A service member is playing basketball, suddenly collapses, and is pronounced dead on arrival upon being rushed to the hospital. Nothing in the person's medical history suggests a life threatening disease. Investigative coverage will be complete (including scene examination and interview of key witnesses, etc.) until the performance of an autopsy. If the preliminary cause of death is determined to be natural, the SAC will conduct a complete review of the investigation. Should the SAC's case review support a manner of death as natural, procedures in section 30-27.3. and 30-27.4. will be followed.

(2) In a second scenario, a service member is found dead in his on-base quarters. Death scene examination discovers white powder around the victim's nose and small amounts of white powder on a table. Field test of the substance determines it to be heroin, and autopsy reports preliminary cause of death as accidental drug overdose. Investigative coverage must be complete and may need to continue beyond the autopsy. Under the UCMJ and some state laws, a person who can be identified as providing the victim with heroin may be charged in the victim's death. Criminal causality cannot be excluded although the manner of death is determined accidental.

30-5.6. Death investigations involving on-base incidents of reported suicide and other self-inflicted incidents (e.g., autoerotic deaths) will be pursued with the same intensity and coverage as known homicides following the appropriate provisions of sections 30-6., 30-27.6. and 30-27.9. Telephonic contact is encouraged between the case agent and the NCISHQ review desk, as such investigations must be reviewed in detail by NCISHQ for potential briefings to the Department of Defense Inspector General (DoD/IG), congressional committees, and families of the deceased.

30-6. GENERAL INVESTIGATIVE PROCEDURES

30-6.1. One purpose of a medicolegal investigation of a death is to establish the cause and manner of death. The cause of death is the disease or injury that directly or indirectly brought about the death, and is established by the forensic autopsy. Manner of death is a medicolegal finding that the death resulted from homicide, suicide, accident, natural causes, or is undetermined, and is primarily dependent on circumstances surrounding the death and autopsy results.

30-6.2. Because staging the death of another person is possible (i.e., making a situation appear to be an accident or suicide), homicide should not be ruled out by an investigator as a consideration, regardless of how obvious it appears that the death scene may point to an alternative manner of death. All medically unattended deaths are to be presumed homicides until investigation proves otherwise, thus preventing destruction or loss of valuable evidence at the scene and loss of important information from witnesses. All logical leads developed and pertaining to any manner of death should be pursued and documented completely. Any evidence of foul play must be further investigated and resolved if possible; contradictory information should be clarified before the close of the investigation. To the extent possible, all discrepancies received from persons interviewed should be resolved through re-interviewing and other appropriate means, since a single interview with persons having pertinent knowledge of the death may not be sufficient and complete. For example, if two people discover a body at the same time yet the details of the discovery differ considerably upon initial interviews with each of the individuals, re-interviews are necessary to resolve major discrepancies in the given accounts. The process of re-interview and thorough documentation minimizes doubt regarding the investigative result, as well as the cause and manner

of death.

30-6.3. NCIS special agents are rarely the first to arrive at a death scene. The deceased is usually discovered by military associates, friends, relatives, or citizens who notify police and medical authorities. Upon notification of the discovery of a dead body or the occurrence of a homicide, the NCIS investigating agent should immediately initiate case notes and record the following data: (1) date and time information received, (2) how notified (telephone, radio, or in person), (3) who made the notification, and (4) details of the scene and incident(s) leading to the death.

a. Upon arrival at the scene, the following data should be recorded in the case notes: (1) time of arrival, (2) the exact location/address, (3) individuals present at scene, (4) weather conditions and temperatures, and (5) other conditions subject to change (e.g., lighting conditions, odors present). The responding agent(s) is encouraged to refer to the NCIS Field Guide to Crime Scene Investigations to ensure complete investigative coverage of the scene. The Field Guide is located on the Lighthouse under Guidelines & References, then Manuals and User Guides. Complete case notes are necessary in preparing the ROI and may later assist the investigating agent in preparing for court testimony. The defense in a murder trial often relies on the timeline in an alibi. Times corresponding to agent notification and the arrival at the scene are frequently the first subjects covered in a cross-examination. Uncertainty surrounding basic and elementary aspects of an investigation may result in the questioning of the accuracy of an agent's perceptions.

30-6.4. Investigating agents should take charge of the scene, ensuring that competent medical authority has pronounced the person dead. If medical personnel have not arrived at the scene, the investigating agent must check for vital signs (pulse, heartbeat, and respiration) to determine if the victim is deceased. An absence of vital signs, as well as an examination of the victim’s eyes and body temperature can establish the death of a victim. Upon death, eyes become clouded and dull and the body is cool to the touch. Additionally, a touch to the cornea of the eyes that does not produce movement or reaction is a probable indicator of death. Obvious signs of livor mortis and/or rigor mortis will also assist in determining if the victim is deceased.

30-6.5. Competent medical authority should be called to the scene to pronounce death in cases where the victim has not been removed from the scene for emergency medical care but is believed to be deceased.

30-6.6. NCIS special agents should inventory victim's belongings for possible evidence and/or investigative leads. This is to be done in conjunction with command inventories of personal effects if the death scene is not the location where the effects are maintained. Careful attention must be given to seizing electronic devices and media, such as computers and computer media, cell phones, and personal digital devices (PDAs). A Cyber Department agent should accompany the investigative agent to assist in securing the electronic evidence without harm to the forensic value.

30-7. DYING DECLARATION

30-7.1. Upon arriving at a scene and discovering a victim is alive, conscious, and receiving treatment, but with potentially fatal injuries, the investigative agent(s) should attempt to interview the victim to obtain a statement, or Dying Declaration. If the victim is removed from the scene for

emergency medical treatment, an agent should accompany the victim in an attempt to complete the interview. A Dying Declaration is an exception to the hearsay rule (Military Rule of Evidence 804 (b)(2) and similar state evidence rules) and may be introduced at trial to identify the individual(s) responsible for the victim's death and circumstances that induced death.

30-7.2. While requirements for legal acceptance vary in different jurisdictions, elements of a Dying Declaration must include the following basic elements:

a. Declarations must be made by the victim under the sense of impending death and without hope of recovery. It is not required for a physician to inform the victim of fatality, only that the victim's actions and speech indicate there is a belief of forthcoming death. The criteria are then met.

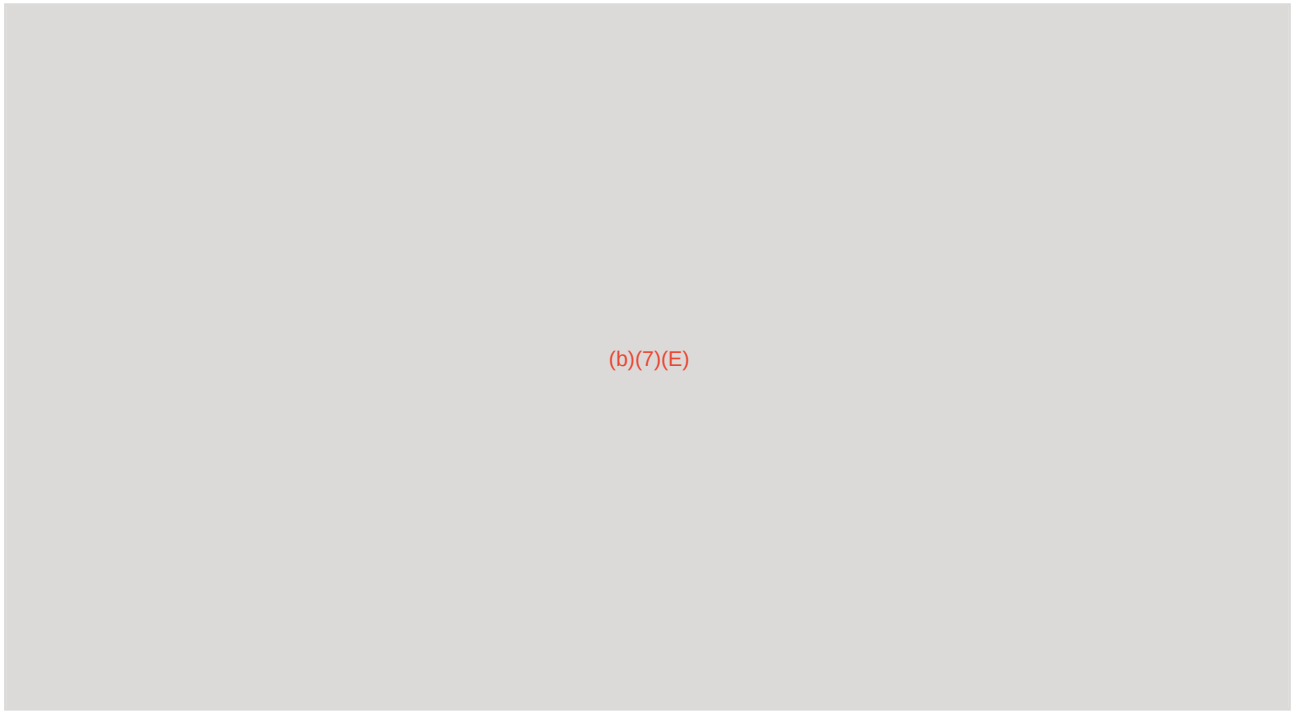
b. Declarations must refer only to the manner and circumstances that precipitated the victim's condition (ultimately death) and if provided, the name(s) of the individual(s) responsible.

c. The victim must die.

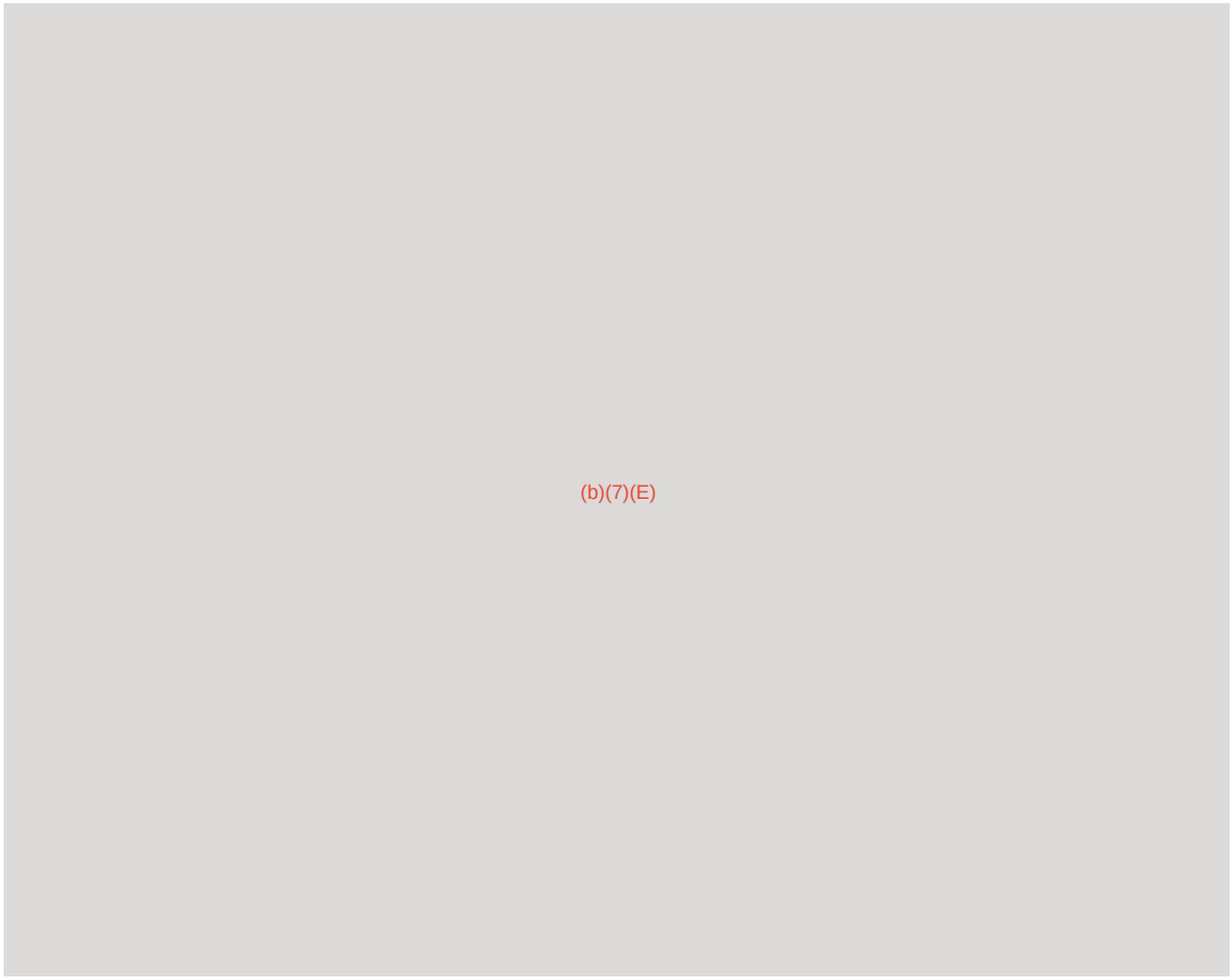
d. Declarations may be used only in a prosecution for homicide, or for any offense resulting in the death of the alleged victim (the declarant).

30-7.3. While not a legal requirement, it is suggested that the victim's oral statement be reduced to written statement form and signed by the victim. No oath or witness is required, but it is recommended that a witness be present if possible. The statement may also be based on intelligible signs, spontaneously or in response to solicitation (including leading questions).

30-8. DEATH SCENE INVESTIGATION

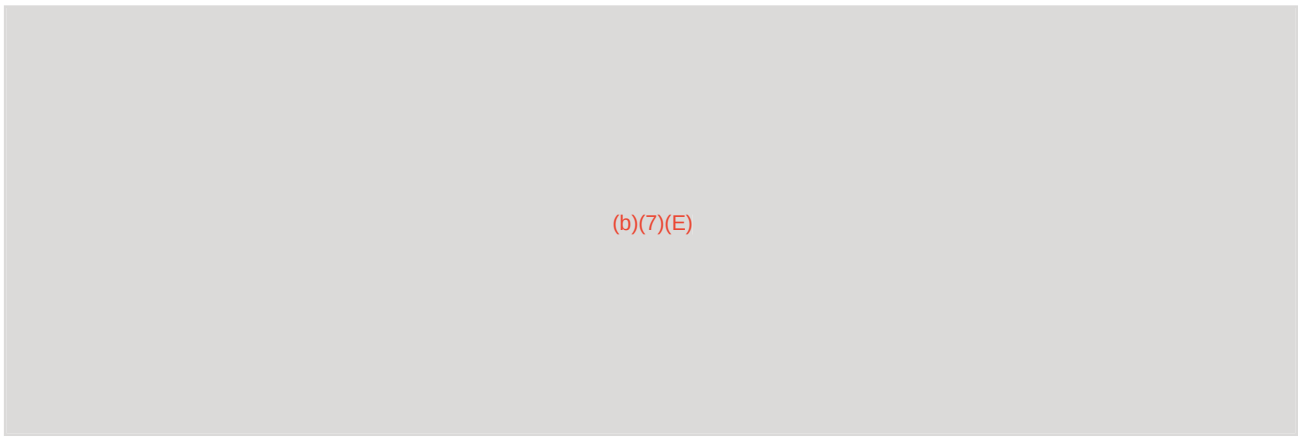


Pages 847 through 850 redacted for the following reasons:
- -
(b)(7)(E)



30-9. INTERPRETATION OF INJURIES

30-9.1. For a more detailed discussion of injuries with which the agent should be familiar at the scene, refer to the NCIS Field Guide for Crime Scene Investigations.



30-9.3. Types of Gunshot Wounds. A bullet passing through a body (perforating wound) produces

wounds of entrance and exit that may be recognized and interpreted by the forensic pathologist. The following will assist the investigating agent in recognizing and interpreting bullet wounds:

a. Entrance Wounds. Typical entrance wounds are round regular holes that produce minimal bleeding. Frequently, the skin's natural resistance is stretched by the impacting bullet and produces a hole that is characteristically smaller than the bullet itself. In many instances there is a reddish brown ring of abrasion around the margin of the wound caused by the bullet's impact. Entrance wounds may exhibit bizarre shapes if the bullet impacts with an intermediate target prior to entering the body. The bullet and other products of the weapon's discharge produce several other characteristics and effects on the skin and clothing of the victim. These marks are indicative of the angle at which the bullet entered the body, as well as the distance from which the weapon was discharged. Wounds inflicted with the gun muzzle held directly in contact with the victim are called contact wounds. Those inflicted with the weapon's muzzle close to, but not touching the victim's skin, are near-contact wounds. Intermediate range wounds entail the muzzle being held away from the body, but close enough for powder particles to be projected into and onto the skin. The only marks associated with a distant wound are those produced by the bullet penetrating the skin. These are general rules, and pathologists may use varied terminology to document such wounds.

b. Contact Wounds. Contact wounds are produced when the weapon is discharged in contact with the victim's body. Hard contact wounds (those inflicted over a bony surface) normally produce large ragged wounds referred to as a stellate wound (star-like) because of the explosive force of gases between the skin and underlying bone produced by the discharge. Skin and tissue surrounding the bullet hole is frequently torn, producing ragged, lacerations radiating outward from the hole. Particles of unburned and partially burned gunpowder and other discharge debris are blown into the wound tract for a distance below the skin's surface. (b)(7)(E)

(b)(7)(E)

c. Near Contact Wounds. It is common to find wounds surrounded by a wide zone of powder, soot, and overlying blackened seared skin. The zone of searing is wider than that seen in loose contact wounds. The soot in the seared zone penetrates the skin and cannot be completely wiped away. Near contact wounds with handguns usually occur at ranges less than one-half inch. This will vary, depending on the caliber, ammunition, and barrel length.

d. Intermediate Range Wounds. These wounds are normally circular with the ring of abrasion around the wound. Normally there is a "tattooing" in the skin around the wound caused by unburned and partially burned gunpowder and other discharge debris projected onto the victim. This generally begins at a muzzle-to-target distance of approximately one-half inch. (b)(7)(E)

(b)(7)(E)

e. Distant Wounds. These wounds are produced when the firearm is discharged at a distance,

allowing for the only marks on the body to be produced by the bullet penetrating the skin. (b)(7)(E) (b)(7)(E) (b)(7)(E) Distant and intermediate wounds may be difficult to distinguish from one another if overlying.

f. Exit Wounds. These wounds are generally larger than the bullet or the entrance wound and are often ragged and irregular in shape. The likelihood of soot and gunpowder in surrounding tissue is remote. Exit wounds generally bleed more than entrance wounds and often have internal tissue protruding from the wound. When a bullet exits an area of the body where there is tight clothing (e.g., belts, tight fitting leather coats, brassieres, etc.) the wound may have the appearance of an entrance wound. This is called a shored exit wound, and in such cases, it is crucial that the body be examined and photographed with the clothing in place to allow the pathologist to accurately interpret the wound.

g. Shotgun Wounds. Shotgun wounds differ in several aspects from those caused by other firearms. A typical contact shotgun wound in areas aside from the head, measures the approximate diameter of the barrel. Marginal abrasion will be evident and the wound edges blackened. Abundant soot and gunpowder may be inside the wound. At loose contact, scorching, soot, and powder residue soiling on the target surrounding the entry wound will be present. Annular abrasions surrounding a shotgun entry wound at a distance of up to one inch are the result of a blow back effect, which stretches the skin around the wound. When a shotgun is discharged from a distance of approximately four to ten feet (depending on the individual weapon, length of barrel, and type of ammunition), the charge strikes in a compact mass. The resulting wound is a large central hole, circular with ragged edges made up of many separate overlapping perforations caused by individual shotgun pellets. This characteristic wound is commonly referred to as the "cookie cutter" effect of a shotgun wound. At this distance, the average shotgun may deposit considerable powder, soot, and smoke soiling the clothing or skin. Beyond ten feet the charge begins to break apart into individual pellets and scatters while in flight and penetrates the body in a more diffused pattern with no central hole. The interior of a shotgun barrel is not rifled; therefore no individual ballistic markings are engraved on pellets fired from the weapon. However, examination of individual pellets by a firearms expert can determine the size of the shot and whether the pellet is either lead or steel. (b)(7)(E)

(b)(7)(E)

30-9.5. Death Involving Stabbing, Cutting, and Chopping. Deaths or injuries inflicted by stabbing, cutting, or chopping are common in cases of homicide and suicide and are often difficult to properly identify and interpret. The following is provided to assist the investigating agent in the recognition and interpretation of these wounds:

a. Stab Wounds. Stab wounds may be inflicted with any object having a reasonably sharp point.

The shape of the wound depends on the direction of penetration, shape of the weapon, and the movement of the weapon while in the wound. A stab wound is identified as one where the depth exceeds the length of the wound. In some instances, the wound may reflect the type of weapon involved (e.g., configuration of a screwdriver or a pair of scissors). The edges of the wound are sharp, straight, and not undermined. The surrounding skin is usually devoid of bruising. Bruising noted in proximity to a stab wound is most likely caused by the impact of the fist or hilt of the weapon. Abrasions along the edges of the wound are usually absent; however, they may be apparent on the margins of the wound caused by the entry and removal of the weapon. A stab wound generally suggests homicidal assault by virtue of its appearance and depth. The amount of blood present at the scene is often minimal, as bleeding may be mostly internal. Suicidal deaths caused by self-inflicted stab wounds may also be encountered.

b. Cutting (Incised) Wounds. An incised wound is inflicted by a sharp-edged instrument, with the length of the wound exceeding the depth. Characteristically, an incised wound appears "clean" and well defined, with a general absence of abrasion around the margin of the wound. The wound edges may be straight or jagged, depending on the shape of the cutting instrument, but edges are not abraded or undermined. The absence of small, thin delicate "bridges" of soft tissue between the sides of the wound is a distinctive characteristic of an incised wound. Guidance regarding self-inflicted incised wounds is set forth later in this chapter.

c. Defense Wounds. Often the investigating agent will observe both stab and incised wounds on the palms, back of the hands, and forearms of a victim. These wounds may be defense wounds inflicted when raising hands in self-defense. Cuts and stab wounds may also sometimes be found on the lower extremities if the victim was lying on the ground, using his legs for defense. Generally, there is no pattern to such injuries and a random collection of incised and stab wounds is revealed. However, superficial cuts in a horizontal, vertical, or large circular pattern on the chest or abdomen may indicate wielding of the knife in front of the victim. Movement of the victim and/or the assailant may cause interruptions in the pattern. The existence of a number of defense wounds may rule out consideration of accidental wounding and is indicative of a struggle.

d. Hesitation wounds. The investigating agent may also observe a pattern of multiple superficial parallel-incised wounds on the wrists, neck, elbows, and ankles of a victim. These wounds may be hesitation wounds which were self-inflicted by the individual while attempting suicide. Often, such wounds are inflicted superficially and are not intended to cause serious harm to the person but rather to gain sympathy. A pattern of this type of wound in various stages of healing is indicative of a person who has contemplated or previously attempted suicide.

e. Multiple Stab Wounds. The existence of multiple stab wounds may show intent on the part of the assailant to inflict grievous bodily harm or to kill the victim. A pattern of multiple stab wounds also helps rule out the possibility of accidental injury to the victim during an argument or altercation.

f. Chopping Wounds. A chopping wound is a combination of a cut and laceration (a blunt force injury discussed later in this chapter). The wound is usually inflicted with a heavy instrument such as a machete, hatchet, ax, or cleaver. These wounds may appear deep and gaping, and may be surrounded by contusions and abrasions. The underlying bone may have received a cut from the

sharp edge of the instrument and may be fractured. The pathologist may be able to determine the type of instrument used by observing the depth, width, and general appearance of the wound. (b)(7)(E) (b)(7)(E) (b)(7)(E) Suicidal chop wounds are rare.

30-9.6. Death by Asphyxiation. Asphyxia is a condition in which the body cannot take in oxygen and cannot eliminate carbon dioxide. Asphyxial deaths may result from homicide, suicide, or accidental means. The following are guidelines for agents investigating deaths by asphyxiation:

a. Strangulation. Strangulation is asphyxiation caused by a constriction or compression to the neck, resulting in the obstruction of blood vessels or air passages, both vital to the function of the brain. It can be manual, ligature, or hanging.

(1) Manual strangulation. A fracture of the hyoid bone (an u-shaped bone at the base of the tongue) is indicative of manual strangulation. A person cannot manually strangulate himself, since at the time of unconsciousness, the hands relax and breathing resumes. The hallmark of manual strangulation is the presence of fingernail marks on the neck. Fingernail marks can be left by the assailant and also may be self-inflicted by the victim during struggle to remove the assailant's grip. (b)(7)(E) Skin and tissue found under the victim's fingernails may be a combination of tissue from both the assailant and the victim. (b)(7)(E) (b)(7)(E) Fingernail marks are encountered in many cases involving manual strangulation; however, the absence of fingernail marks on a victim's neck does not rule out the possibility of strangulation. Manual strangulation may also be achieved by the use of a chokehold, arm bar control, and/or carotid sleeper hold. Injury of the skin as a result of such techniques is usually absent; therefore, the investigative agent should be familiar with associated injuries in the case of questioned strangulation.

(2) Ligature. Strangulation by ligature (garroting) occurs when the pressure on the neck is caused by a constricting band that is tightened by a force other than body weight. The ligature is often an item readily available at the scene (e.g., belts, electrical cords, laundry rope, panty hose, and other items of clothing) and may leave a pattern injury on the victim's neck. Frequently, a positive comparison between the ligature and the resultant pattern injury can be made and the ligature should generally leave a horizontal furrow or groove around the victim's neck. Strangulation by ligature is indicative of a homicidal killing.

(b)(7)(E)

(3) Hangings. Hanging is a type of strangulation executed by means of a rope, cord, or similar ligature tightened by the weight of body. Note that a person does not have to be completely suspended to die from hanging and may take place in any position where pressure on the neck is maintained above that necessary for vascular occlusion. Hanging usually leaves definite and readily recognizable evidence, even after the individual has been cut from the ligature and the scene altered

to suggest a different type of death. The furrow or groove around the victim's neck may suggest the type of loop used and the weave pattern of the ligature (especially in cases where a rope is used) may be imprinted on the skin permitting a match of patterns. In a typical hanging case, the arms of the noose pass around the neck and upward toward the knot, forming an inverted "V" on the knot's side. An abraded area of skin often marks the point of suspension. In addition to the mark produced by the noose (knot), bizarre abrasions and bruises are occasionally seen on the victim's neck. Such may be the case in which constriction of the neck by the noose causes pinching of the skin and the vertical folds that rub against the noose become abraded. At times, blisters may result from friction of a tight noose; however, if the loop is made of soft materials such as a towel or scarf, a noticeable furrow may not be apparent on the neck. Scattered pinpoint hemorrhages are often noted on the face of a hanging victim particularly in the conjunctiva and sclera, but it should be noted that petechial hemorrhages are NOT conclusive evidence of death by hanging. Identical hemorrhages are often found in cases of natural death with marked facial lividity or found following cardiopulmonary resuscitation, independent of the mechanism of death. The tongue may protrude from the mouth of a hanging victim. In order to enable subsequent examination of the ligature, the knot should not be untied. Removal of the ligature/noose from the deceased should be done by cutting the noose away from the knot and then tying the ends with string or wire. Many forensic pathologists prefer that the ligature is cut at the point of suspension and the noose is left on the victim for later examination and removal at the time of autopsy.

b. Autoerotic Deaths. An agent may encounter various types of accidental asphyxia associated with sexual perversion. Many of these deaths are discovered under bizarre circumstances, perhaps suggesting foul play. The death scene is normally a secluded area, which may be indoors or outdoors, and the door to the area is commonly locked from the inside. While in many instances the victim is a young male, possibly married with a family, there have been cases of female deaths that have been incorrectly attributed to homicide or suicide. The victim may be found hanged, strangled, or with a plastic bag over the head. Generally when a noose is used, it is padded with soft material to preclude marking of the neck. In cases where the victim's hands and feet are bound behind the individual, the body is self-tied making release not usually difficult. Binding of the extremities, tying of the wrists or handcuffing is common. Contrary to expectation, the genitals are not necessarily exposed, and sometimes the body may be found clothed in female attire (particularly underwear). Pornographic photographs or similar material may also be found at the scene within view of the deceased. Individuals engaging in this activity are believed to feel a reduction of the blood supply to the brain, stimulating and heightening sexual response. Death associated with this activity is usually considered to be accidental, as the deceased did not intend to contribute to his or her own death. Note that the death scene may have been altered by friends or relatives to conceal the embarrassment of a bizarre autoerotic death. Another factor to consider is the method of self-rescue (escape mechanism), with many deaths normally resulting from failure of this mechanism, which could be as simple as standing up. The agent should search for evidence of repetitious previous experiences, including rope abrasion over doors, beams, etc., as well as a cache of clothing or paraphernalia associated with autoerotic practices.

c. Drowning. The investigating agent should be aware that current forensic medicine does not include a reliable test that presents an unequivocal diagnosis of drowning. Investigation in drowning cases demands a thorough examination of the scene and interview of witnesses who can provide information regarding the victim's activities that lead up to the drowning. Often,

accidental drowning is associated with alcohol or drug intoxication where the victim accidentally falls into the water and drowns. In some cases, death in the water is due to natural causes, such as a heart attack or cerebral hemorrhage during bathing or swimming. In some cases the presence of pale or pale-red foam in the victim's mouth and nose may be indicative of drowning. Suicidal drowning in bodies of water and bathtubs are also possible but may be difficult to distinguish from accidental drowning unless suicidal motivation is determined. Although a weighted body may suggest foul play, an individual committing suicide may also weight one's body to hasten drowning and prevent recovery. In such cases, careful examination of weighted bodies must be made for injuries potentially suggesting homicide or violence, and for self-inflicted injuries such as slashed wrists. Binding and weighing arrangements must be examined to determine if the victim conceivably accomplished the act alone. Homicidal drowning is rare and is usually accompanied by signs of physical violence. The forensic autopsy is the key factor in determining if a drowning resulted from suicide, homicide, or accidental means, and it is important that the pathologist be apprised of all aspects of the scene and other investigative results known to the agent at the time of autopsy. Drowning where the victim's body is not recovered shall be initiated under the Missing Person Case Category (7M) until such time as the body or remains are recovered or a competent Navy Authority (Command/BUPERS) issues a DD Form 1300 (report of casualty or "statement of death" equivalent to a death certificate). At such time upon receipt of the certification of death, the investigation will be changed to a Death investigation (Category 7H). A National Crime Information Center (NCIC) entry will be made under a missing person in such cases and removed in case where the remains are recovered at a later date.

d. Smothering. Blockage of the nose and mouth (external airway) causes death by asphyxiation due to the inability to breathe. This may be accomplished by holding a pillow over the victim's face or other means by which the victim's external airway is blocked. The use of gags in the internal airway (such as the mouth) is considered choking vice smothering. Gags should not be removed from a deceased victim until the forensic pathologist can evaluate the extent and location of the obstruction. (b)(7)(E) (b)(7)(E) Identifying this type of death is often exceedingly difficult, calling for close liaison between the investigating agent and the pathologist. The presence of hemorrhages and tears inside the victim's mouth (especially the inside of the lips and cheeks) are indicators that force was applied to the victim's face, suggesting manual smothering. In such a case, bruises and abrasions to the cheeks and chin may be significant and may be suggestive of trauma to the face. Smothering by placing a plastic bag over the victim's head may also suggest suicide, but the presence of evidence revealing glue sniffing and inhalation of other vapors and aerosols while a plastic bag is placed over the victim's head is a common practice. Water vapor accumulates in the plastic bag, which contains the glue or aerosol and contributes to the adherence of the plastic to the skin, sealing off outside air. Deaths associated with inhalation of aerosols (huffing) without the use of plastic bags are also known, and these individuals use paper bags and towels into which an aerosol is directly applied. Such deaths are usually accidental, and toxicological examination of biological samples obtained during autopsy may detect the presence of the substance inhaled by the victim.

e. Carbon Monoxide Deaths. Carbon monoxide causes asphyxiation by blocking the blood from carrying oxygen to the body. Carbon monoxide is an odorless, colorless, non-irritating gas, and

many suicidal and accidental deaths result from carbon monoxide poisoning. A common mode of suicide is for the victim to connect the exhaust of an automobile into the vehicle passenger compartment, allowing the victim to inhale the exhaust emissions until unconsciousness and eventual death occurs. Many accidental deaths occur due to faulty exhaust systems in vehicles, allowing exhaust emissions to seep into the passenger compartment, or from malfunctioning heating devices in living quarters. Note that alcohol, barbiturates, sedatives, and numerous other drugs are factors that increase the toxic effect of acute carbon monoxide poisoning. Investigation in these cases should include inspection of the device suspected of malfunctioning by an expert and a thorough examination of the death scene by the investigating agent. A telltale sign of carbon monoxide poisoning is a bright cherry red discoloration of the skin, the blood, and the livor mortis (discussed later in this chapter). The fingernails are also involved in providing telltale signs of deaths associated with carbon monoxide poisoning and are usually discolored purple. However, cyanide poisoning and exposure of the dead body to a cold and moist environment may cause redness indistinguishable from that due to carbon monoxide. Likewise, with lower concentration the color may go unnoticed. An autopsy generally establishes that death resulted from carbon monoxide poisoning in these cases.

30-9.7. Blunt Force Injuries. Blunt force injuries are the result of falls, collisions, or blows with blunt instruments or surfaces. Wounds produced by blunt force are generally characterized by tearing, shearing, or crushing of tissue, bone, or internal organs. Extensive bleeding into adjacent soft tissue is the general rule. These injuries may or may not indicate a struggle and must be carefully examined and interpreted by the agent and the pathologist. The three basic types of blunt force injuries are detailed below:

a. Contusion (Bruise). A contusion signifies hemorrhage into the skin or subcutaneous tissue or both. It results from a blow or compression that crushes the soft tissue and ruptures blood vessels but does not break the skin. The presence of contusions may indicate the victim engaged in a struggle. However, the investigating agent should be cognizant that not all application of blunt force causes a contusion and contusions may be inflicted on a body after death. Additionally, the instrument used to inflict the contusion may be identified from the injury itself. Often the pattern of the injury mirrors the instrument (e.g., belt buckle, length of wire, nightstick, etc.) and recognition of the pattern may help in reconstruction of the circumstances of injury. Bruises change color over time in a general progression and generally, the color of a bruise changes from light bluish-red to dark purple, green, yellow, and then brown. This change proceeds from the periphery of the bruise toward its center and vice versa. Thus, a discolored bruise with pale center is likely to be at least several days old, depending on a number of factors. Microscopic examination for aging of a bruise is generally recommended for a more accurate evaluation.

b. Laceration. A laceration is a tear produced by a blunt force trauma. The force and its direction determine the appearance, depth, and associated injury. A laceration may result from a perpendicular blow with a relatively broad object (such as a hammer or by falling onto a hard surface) or by a glancing blow, tearing only the skin. A laceration may be external, with tearing of the skin and tissues, or internal, where organs are ruptured, split, or fragmented. A laceration on the external portion of the victim's body should not be confused with an incised wound as a laceration has the following characteristics: abraded margins, ragged edges, and bridging of blood vessels, nerves and connective tissue.

c. Abrasions. An abrasion is caused by a scraping of the skin sufficient to remove its superficial layers. Often it is possible to determine the direction and the manner in which the scraping occurred. Depending on the mechanism of the abrasion, it may be called a graze (where a bullet scrapes the skin), a scratch that is caused by a scraping edge or fingernail, or a brush burn caused by the friction of rubbing against a rough surface. Like contusions, abrasions may be inflicted on a body after death. Since abrasions are often characteristically patterned, the nature of the force and instrument involved may be identified by the pathologist and may be crucial in interpreting the circumstances surrounding the victim's demise. For example, abrasions on one side of the victim's head may be suggestive of a fall, while abrasions to both sides of the head and face may be suggestive of blows and an altercation.

30-9.8. Drug Related Deaths. Investigations of deaths believed to be connected to drug abuse consist of three basic components: (1) investigation at the death scene, (2) the autopsy, and (3) the toxicological investigation of biological samples collected by the pathologist. The proper interaction between the investigating components and the scientific community is necessary for the successful solution of drug-associated deaths. In all cases of suspected drug abuse the scene must be carefully examined and photographed. The search of the scene and the deceased should be directed towards location of drugs and drug related paraphernalia. The search of the deceased, whether done at the scene or at the morgue/mortuary should include detailed examination of the clothing and all personal items which may lead to the identification of the individual from whom the deceased obtained drugs. A search of the body by the pathologist should include examination of all body orifices where a drug could be secreted. In cases of suspected injection, the needle or syringe and tourniquet may be found in place on the body. Blood may be occasionally found in the syringe due to intentional aspiration and reinjection of the blood. This confirms that injection was made into the blood stream. The tourniquet itself should also be examined as an area of possible drug concealment.

30-9.9. A search of the scene and surrounding areas should be conducted for drugs and paraphernalia. The paraphernalia may include syringes, tourniquets, bottle caps, and spoons used as cookers. Any prescription pill bottles and other containers suspected of containing or having contained any drugs should be seized as evidence, and all drugs and paraphernalia should be submitted for laboratory examination. In those cases where the pathologist does not inspect the death scene, the investigating agent should brief the pathologist about the death scene investigation and any drugs located before the autopsy is conducted. In particular, the pathologist should be advised of what types of known or suspected drugs were observed and seized at the scene, and of any pertinent information regarding drug abuse which may have been obtained from interview of witnesses. In addition to searching the death scene for drugs and related paraphernalia, an examination of the scene and its immediate surroundings should be expanded to document those items suggestive of drug abuse. The following observations may be suggestive of drug abuse on the part of the deceased:

a. Filthy surroundings with partially eaten food;

b. Presence of psychedelic posters, pharmaceutical information, and literature on folklore medicine; or

c. Presence of antacids and laxatives (especially milk of magnesia).

30-9.10. The mere fact that a body is found in a certain location does not preclude the possibility that the body has been moved, either before or after death, from the location where drug injection occurred. In incidents where group narcotics activities may have occurred, consideration should be given to the possibility of "dumping" by the others in the associated group. A result of moving and dumping the body may be the inflicting of abrasions or contusions on the body of the deceased, which may lead the investigating agent to hastily conclude that a homicide has occurred. The position of the body and observation of rigor mortis and livor mortis (body changes that occur after death are discussed later in this chapter) may be helpful in determining the time of death and whether the body was moved. Needle marks, abscesses, scars, and tattoos (applied to cover injection sights) may be observed on the deceased during the examination by the pathologist and investigating agent and should be photographed. Once the death scene examination is complete, the investigating agent must continue to liaison with the pathologist to determine the results of autopsy and toxicological examination of biological samples obtained at the time of autopsy. Investigation should be continued in an attempt to identify the source of illicit narcotics contributing to the victim's death. If the supplier of narcotics to the deceased is identified, the investigation should then shift to establishing the individual's culpability in victim's death.

30-9.11. Thermal Injuries. Thermal burns are noted as a cause of death. While most burns related to deaths encountered by NCIS are accidental (e.g., fire in living quarters or automobile accident related), the investigating agent should be conversant with death caused by thermal injury. Burns are commonly classified according to the depth of tissue destruction as follows:

a. First Degree. Burns are superficial and the damage is limited to the outer layer of skin. Blisters do not form, but peeling may follow. The burned area is red, swollen, and painful.

b. Second Degree. Burns typically show blistering and the upper layers of skin are destroyed.

c. Third Degree. The entire thickness of the skin is destroyed. Pain is usually absent because nerve endings in the skin are destroyed.

d. Fourth Degree. More severe injuries such as charring and complete destruction of the skin and underlying tissue.

30-9.12. The severity of burn injuries depends directly on the intensity of the heat and duration of exposure. While some chemical fires may reach several thousand degrees, the ordinary house fire seldom exceeds 1200 degrees Fahrenheit; hence, it is unlikely that the body of an adult will burn completely in a house fire. (b)(7)(E)

(b)(7)(E)

(b)(7)(E) Obesity and clothes contribute to faster and more complete destruction of a body in a fire. The body of a fire victim is often discovered with the hands, arms, and legs in a defensive position much like that of a boxer, and is referred to as the "pugilistic attitude or position". This position does not refer to the victim's posture prior to death, but rather is caused by contraction of muscle tissue brought on by the fire. (b)(7)(E)

(b)(7)(E)

(b)(7)(E) The thrust of investigation in fire related deaths should be directed towards establishing circumstances/origin of the fire, positive identification of the victim, and determination of the cause of death. Often, in establishing the cause of death, the pathologist may be able to establish if the victim was alive at the time of the fire. The presence or absence of soot in the airway, as well as carbon monoxide levels in body tissues, assist the pathologist in making these determinations.

30-9.13. Electrocution. Deaths due to electrical injuries are infrequently investigated by NCIS. However, the circumstances surrounding these deaths are often not readily apparent and require detailed investigation. The passage of electric current (low or high voltage) through the human body is capable of producing a wide variety of effects ranging from an insignificant localized muscle spasm with little or no contact burn to the skin to instantaneous death accompanied by severe burning on the victim's body. These investigations require a comprehensive death scene investigation and interview of all pertinent witnesses. The investigation must also call for consultation with an expert witness (electrical engineer or maintenance officer) who can identify and explain all electrical lines, cables, or equipment in the area that may have contributed to the victim's death. Where the death is associated with an electrical device or appliance, the device must be seized as evidence and forwarded to a laboratory for examination to determine if device malfunction caused electrocution of the victim. Victims of electrocution may remain conscious and speak or move for several seconds, and even unplug or disable the offending appliance after a fatal electrical shock. Deaths from lightening often display a reddened area in a fern like appearance on the body.

30-9.14. Death Involving Poisons. Death resulting from poisoning is not often investigated by NCIS agents. However, an investigating agent may encounter an unexplained death resulting from homicide, suicide, or accidental poisoning. The agent can be called to investigate the accidental poisoning of a dependent child. A poisoning is generally defined as any substance, which when introduced into a living organism, causes detrimental or destructive effects. Investigation of cases involving suspected poisoning is a joint effort involving the investigator and pathologist. An investigation is often requested after the victim seeks medical assistance complaining of illness and dies after not responding to medical treatment. In such cases, acquisition of all medical treatment records and the interview of all attending medical personnel are mandatory. In cases where the poisoning may have occurred at the victim's residence, living quarters must be examined with emphasis directed toward location and seizure of all toxic substances and any items uniquely identified as being poisonous in nature. Ethyl glycol (anti-freeze), a sweet tasting poison commonly found in the home, has been identified in suicides and accidental deaths; homicides should also be considered. If the pathologist does not visit the death scene, the agent should provide a thorough description of any questionable items discovered at the scene, submitting all suspect materials for laboratory examination and identification.

30-10. TIME OF DEATH AND CHANGES AFTER DEATH

30-10.1. If the circumstances surrounding a death are unknown, an estimation of the time of death may represent an essential contribution in reconstruction of the circumstances surrounding the death. For a more detailed discussion of estimating the postmortem interval, the agent(s) should

refer to the NCIS Field Guide for Crime Scene Investigations. There is no single independent reliable method for determination of the postmortem interval. This determination consists of an opinion offered by the pathologist based on his observations of the deceased and those recorded at the time of autopsy coupled with information provided by the death scene examination and interview of witnesses. An exact determination of the time of death is usually not possible and the investigating agent must note that such a determination is an estimate and is dependent on multiple variables. The estimation of postmortem interval begins with establishing a window of time between when the person was last known to be alive and when the body was discovered. A body begins to decompose at the time of death and continues through various recognizable stages depending on several variables that include:

a. Temperature of the environment in which the body is located;

b. Time interval since death;

c. Location of the body (e.g., in water, above or below ground);

d. Humidity and air currents;

e. Body stature and condition prior to death; and

f. Activity of the victim just prior to death.

30-10.2. As previously detailed in this chapter, a thorough examination of the death scene coupled with interviews of witnesses may significantly contribute to establishing a realistic estimate of the time of death. There are several recognizable postmortem changes that the investigating agent should recognize and understand, such as immediate changes that include cessation of respiration and circulation, skin pallor, muscular relaxation, and fixed and dilated pupils. This is followed by early postmortem changes that include:

a. Postmortem Body Cooling (Algor Mortis). After death, the living body temperature of 98.6 degrees Fahrenheit decreases and starts equating with the cooler environmental temperature. It is highly desirable for the pathologist (or other competent medical officer) to be called to the death scene to record the body temperature and other observations. Be aware that body cooling is affected by many variables such as ambient temperature, environmental conditions, clothing, and amount of fat tissue.

b. Rigor Mortis. The process of rigor mortis is the result of a stiffening of body muscles as a result of chemical changes in muscle fibers at death. As a general rule, rigor mortis begins to appear two to four hours after death and is first noticeable in the short muscles such as the neck and jaw. The process generally progresses from the short muscles in the neck and jaw to the long muscles in the upper and lower extremities. Rigor mortis is usually complete in six to twelve hours to which the jaws, neck, torso, upper and lower extremities are in a state of marked stiffening and resist any movement in those body parts. This complete state of rigor begins to disappear after approximately 18 to 36 hours after death and is usually gone after 48 hours. Be aware that many factors can affect the onset and disappearance of rigor mortis. Rigor mortis can be broken by

manipulation of the muscles but can reappear if the rigor is interrupted before total completion. When the appearance of rigid limbs is inconsistent with gravitational forces, rigor is a reliable indicator of a postmortem change in position of the body.

c. Livor Mortis. Livor mortis results from the postmortem pooling and settling of blood within the blood vessels due to gravitational forces. Livor mortis is recognized by the deep maroon to purple discoloration of the skin on the deceased. Location of the livor mortis is determined by position of the body at the time of death. In a body suspended by a ligature around the neck, the livor mortis would form in the lower extremities (lower portion of the arms and feet). In a body laying face down, the livor mortis will form in the frontal aspects of the body. Similarly, the body positioned on the shoulder and buttocks on a flat surface will demonstrate livor mortis in the back. The onset of livor mortis begins approximately 30 minutes after death and becomes fixed after approximately six to twelve hours. The term "fixed" means that after the livor mortis has settled in one position, it can no longer be significantly shifted by a change in the body position. This can be significant to the investigating agent observing a body in a position inconsistent with the positioning of the livor mortis, indicating movement of the body after death. Additionally, recognition and interpretation of livor mortis assists in estimating early postmortem interval. The color of the livor mortis may also be significant to the investigating agent and the pathologist as the following general guidance has been established in forensic pathology:

(1) Cherry red coloration may denote antemortem exposure to carbon monoxide. This coloration may also be a result of cyanide and fluroacetate poisoning.

(2) Bodies recovered from water or exposed to cold temperatures may develop cherry-pink livor mortis.

(3) A deep purple hue is observed in the livor mortis associated with asphyxiation or heart attack deaths.

30-10.3. The investigating agent should also be aware that the livor mortis may fail to develop or be difficult to discern in some cases regardless of the body position. This generally occurs in deaths resulting from severe anemia or extreme loss of blood, as in some gunshot wound or stab wound related deaths.

a. Late Postmortem Changes. The investigating agent may also encounter bodies in later stages of postmortem changes. Decomposition is one of the late postmortem changes and is brought about by autolysis (the action of digestive enzymes in the body) and putrefaction (bacterial action throughout the body). Decomposition depends on many factors including the deceased's state of health at the time of death and environmental conditions where the body is located. While each case may differ, the following observations have been established in forensic pathology:

(1) Decomposition is generally observed as a green/blue discoloration in the lower abdomen.

(2) "Marbling" of the skin begins after about 24 hours.

(3) Blistering and bloating may be noted.

(4) Skin slippage depends on environmental conditions and may include the slipping of the "glove" from the hand of the deceased. Gloves often yield a full set of fingerprints and should be properly retained for identification purposes.

(5) Hair and the finger/toenails of the deceased may fall from the body.

(6) Other late postmortem changes include the presence of adipocere (a soapy white substance covering the body), mummification, and skeletonization. Observation of insect activity may also be made on decomposing bodies. Certain forms of flies and other insects deposit eggs on decomposed bodies may develop into maggots. Samples of insect growths can be examined by an entomologist who may be able to estimate the age of the sample. This investigative aspect may further assist the agent and pathologist in establishing the time of death.

(7) Postmortem Injuries. The investigating agent may encounter dead bodies exhibiting injuries which may have occurred after death and require interpretation and explanation by a pathologist. Postmortem injuries may be caused by the action of insects, wild and domestic animals, marine life (in cases where bodies are found in water), and other factors which impact on the body. Injuries may appear to have resulted from violence/trauma before death. Bodies submerged in water often show the effects of mutilation by fish and other marine life or other injuries caused by movement of the body brought about by currents and contact with submerged objects.

30-11. DEATHS INVOLVING INFANTS AND CHILDREN

30-11.1. The investigation of deaths involving infants and children can be grouped into five basic categories: (1) sudden unexplained infant death; (2) accidental; (3) battered child deaths; (4) infanticide; and (5) child neglect deaths. Investigation of these deaths confront the investigating agent with a complex problem which requires complete coordination between the investigating agent, the pathologist, medical authorities, social welfare agencies (the Family Advocacy Program (FAP) Representative (USN) or FAP Manager (USMC)), and legal authorities. All control cases involving deaths of infants and children under the age of 18 will be reviewed by the NCISHQ Death Review Board (DRB) for authorization to close. Additionally, the Under Secretary of Defense directs each service to report suspected or known domestic violence or child abuse fatalities, within 72 hours of receipt of the information. The information is required to be reported using Department of the Navy (DON) Child Abuse and Domestic Violence Fatality Initial Notification, DD Form 2901. Sections 30-21.11 in general and 30-21.11 d. specifically provide further guidance. An unattended child death work sheet is provided as Appendix (4) (NCIS Form 5580/77). For the electronic version of the work sheet, access Lighthouse, and got to Forms Library.

a. Sudden Infant Death Syndrome (SIDS). SIDS is defined by the Centers for Disease Control and Prevention (CDC) as the sudden death of an infant under one (1) year of age which remains unexplained after a thorough investigation, including a complete autopsy, examination of the death scene, and review of the clinical history. Sudden, unexplained infant deaths (SUIDs) are those for which no cause of death was obvious when the infant died. SIDS (also known as crib death) is the

most frequently determined cause of SUIDs. The risk of SIDS peaks at 2-4 months. SIDS is uncommon during the first month of life and after the sixth month of life. About 90% of SIDS cases occur in children under six months of age. SIDS is often referred to as "crib death" since most deaths of this nature occur in the infant's crib. The medical community in general and the forensic medicine discipline in particular has not been able to totally explain this phenomenon. Investigation of deaths of this nature should be directed towards ruling out child abuse/battering or foul play, especially with repeated episodes of SIDS within a family. A thorough death scene examination and careful examination of the results of autopsy are extremely important. Additionally, the medical history files of the infant must be acquired and presented to the pathologist. Unfortunately, deaths resulting from abuse are sometimes misdiagnosed as SIDS, and therefore require extreme care to avoid compounding any errors. Care should be exercised in that concern for the family and pursuit of the truth are complimentary.

b. Accidental death removes SIDS as a consideration. Cribs, beds, mattresses, and bedding are often associated with accidental deaths of children. Widely placed bed slats or side rails can cause accidental smothering or suffocation. Soft mattresses, large waterbeds, or plastic sheets can obstruct the baby's airway. Toys, pacifiers, and bed connections must be examined closely. The individual who initially discovered the child should be interviewed to document the exact location where the body was found and its position at the time of discovery. This information could render evidence that may support or disqualify the notion of respiratory compromise. In addition, the death scene should be examined expeditiously since marked environmental hypothermia or hyperthermia may have affected the child's metabolic functions. A poorly kept home may suggest economic circumstances that compromise adequate nutrition or care.

c. Battered Child Syndrome. Often a child discovered dead at home or brought to an emergency medical center for treatment is observed by attending medical personnel to possess indicators of a history of abuse prior to death. When child abuse is suspected, a significant element of the investigation is the autopsy documenting a history of battering or abuse. Further guidance regarding child sex abuse is available in NCIS-3, Chapter 34, section 34.2. The significant observations that indicate battering or abuse are:

(1) Multiple skin/soft tissue injuries,

(2) Multiple bone injuries,

(3) Long bone injuries in various stages of healing,

(4) Indications of twisting/separations at the joints,

(5) Unexplained head injuries,

(6) Presence of unexplained burns (cigarette burns or scalding produced by submersion in hot water),

(7) Indication of sexual abuse/assault,

(8) Presence of human bite marks, and

(9) Laceration inside the mouth possibly caused by slapping or hitting the child in the face or the child biting himself when battered.

d. Infanticide. Infanticide is the willful killing of a child aged between birth and one year of age. Infanticide usually occurs in two major forms. The first is the abandonment in such places as garbage receptacles, washrooms, public refuse dumps, and secluded areas. Such cases may occur when the infant is allowed to die at the mother's home, in an automobile, or another location where the mother intends to dispose of the body at a later time. The second type of infanticide involves a parent actually killing the infant. The most common means involve various types of asphyxial deaths as outlined earlier in this chapter. Methods include smothering, cupping the hands over the infant's nose and mouth, and drowning. (b)(7)(E) (b)(7)(E) (b)(7)(E) The key to solving such complex cases is often a result of constant coordination between the investigating agent, servicing forensic consultant, and the pathologist. Another essential element of investigations of this nature include in-depth interviews of family members, neighbors and acquaintances, and any individuals possessing knowledge of the child may have been subjected to neglect or abuse.

e. Child Neglect Deaths. Some deaths of infants and children involve cases of severe neglect resulting in the failure of the child to thrive. Children denied life necessities (e.g., food, water, shelter, and clothing) are often medically neglected. Poor nutrition and radiology and/or toxicology may also reflect previous illnesses or injuries. Agents should document all remarkable/unremarkable observations by photography and records/reports.

30-11.2. Investigative Procedures. In all medically unattended child death cases, several elements of investigation must be accomplished. In addition to parents and caregivers, the individual(s) first aware of the death involving a child includes: (1) doctors, (2) hospital emergency personnel, (3) fire department paramedic personnel, (4) local/military police officials, and (5) neighbors. An in-depth interview of all individuals discovering the child, administering emergency medical care, and/or are knowledgeable of any abuse or maltreatment afforded the child is needed. Appendix (4) (NCIS Form 5580/77) also provides a guide to investigating child death cases.

a. Autopsy. In all cases, the investigating agent must ensure that a complete autopsy is conducted. Full body X-rays and photographic coverage of all external and internal injuries is mandatory. Where sexual abuse/assault is suspected, the investigative techniques utilized in rape cases should be employed.

b. History. A primary investigative element should include determination of the age of the child, as well as a determination of the time of death, the general state of health of the child, when the child was last fed or administered medication, and a history of any medical/mental disorders.

c. Medical Review. A review of the child's medical record should be undertaken with the assistance of a competent medical authority to officially document a history of treatment of frequent or unexplained injuries. A review of sibling's medical records or the records of both parents may

also reveal a pattern of violence.

d. Contact with Social Welfare Agencies. The agent should determine any history of suspected or known child abuse and neglect directed against the deceased or any sibling in the deceased's family. The Family Advocacy Program Officer at the local Naval hospital may be able to furnish such information. Additionally, any history of marital discord, mental disorder, or drug/alcohol abuse of the deceased's parents must also be determined.

e. Viewing Living Quarters. The investigating agent and the pathologist should examine the death scene or the victim's residence. The general state of cleanliness and living conditions should be noted, and the condition of the living quarters should be documented through photographs, sketches, and notes in all cases.

f. Neighborhood Inquiries. Inquiries should be conducted in the neighborhood for any indication of abuse or neglect directed towards the deceased or any other member of the child's family.

g. Interviews with babysitters, day care center personnel, or others charged with custody and care of the deceased should be conducted. The investigating agent should note the possibility of batter or abuse by a babysitter or other person charged with temporary care of the deceased.

h. Parents. The investigating agent should obtain the history of events from the parents early in the investigation. Caution must be exercised in investigating a case indicative of the death of a child due to neglect, abuse, or batter, as it requires that the parent(s) be treated as a suspect and potentially requires the advisement of a suspect's constitutional rights.

30-11.3. Other Considerations

(b)(7)(E)

c. The absence of injury on siblings does not preclude single episode lethal abuse. The absence of old injury also does not rule out abuse.

d. Many child abuse injuries, such as broken ribs or other internal injuries, are not readily apparent and require X-ray examination to visualize injuries.

(b)(7)(E)

f. Many health care professionals and investigators do not want to believe that a parent or childcare provider would harm a child, tending to attribute the death to SIDS or other medical explanations rather than suspect a child was killed.

(b)(7)(E)

(b)(7)(E)

30-13. SUICIDE. SECNAVINST 5430.107 series directs that a NCIS investigation will be conducted regarding the unattended death of military personnel, dependents, or DON employees occurring on a Navy or Marine Corps installation where criminal causality cannot be firmly excluded. In all instances of unattended death on a Navy or Marine Corps installation or vessel, the possibility of foul play always exists. Therefore, NCIS should conduct an investigation even in those instances where the death appears from the outset to have resulted from suicide.

30-13.1. Investigation of reported suicide should be investigated under Case Category 7H. When NCIS is requested to investigate attempted suicide, investigation should determine if the individual involved has a security clearance and access to classified material. The matter should be investigated as Case Category 7X investigation to fully document the matter and determine the individual's involvement in intentional self-inflicted injury (Article 115 Malingering, UCMJ). In all investigations with national security ramifications, an information copy of all case documentation must be furnished to the NCISHQ Counterintelligence Directorate, Code 0022.

30-13.2. Security Ramification of Attempted or Actual Suicide. The current DON Information Security Program Regulation (SECNAVINST 5510.36 17MAR99) provides the following guidance regarding incidents of attempted or actual suicide by members of the DON:

a. When a member of the DON who had access to classified information commits suicide or attempts suicide, the commanding officer shall immediately forward all available information by the most expeditious means to the nearest NCIS office for action. The report shall, at a minimum, set forth the nature and extent of the classified information to which the individual had access and the circumstances surrounding the suicide or attempted suicide.

b. The NCIS office receiving such a report shall confer with the commanding officer to coordinate investigative action; and if the NCIS office elects to assume immediate investigative cognizance, command investigative efforts shall be subordinated.

30-13.3. Investigation of suicide or attempted suicide wherein the victim had access to classified material must address two major considerations:

a. The circumstances of the death or the attempt, and

b. The security ramifications. The act of suicide or attempted suicide connotes a serious psychological problem on the part of the individual involved. Historically, a person involved in espionage or other mishandling of classified material may attempt or commit suicide as a result of real or imagined fear of detection or feelings of remorse. In addition to documenting the circumstances of the death or attempted suicide, investigation must include a thorough investigation

of the person's activities and associates. Further, pertinent investigative interests including the command inventory of all classified material accessible to the individual involved must be documented.

30-13.4. Suicide Investigative Procedures. Investigation where suicide is suspected should be done in the same thorough manner as any other death investigation. Homicide may potentially be masqueraded as a suicide and may only be detected by a complete investigation. The pathologist should be requested to conduct a preliminary investigation at the death scene along with the investigating agent. If the pathologist cannot visit the death scene, the agent must discuss the results of the preliminary investigation and other findings with the pathologist even when suicide appears likely at the onset of the investigation. The investigating agent should attend the autopsy and discuss the results of his investigation with the pathologist.

30-13.5. The following investigative procedures should be employed in reported suicide investigations:

a. Death Scene. The death scene should be processed in the same manner as other death investigations. In addition to standard scene processing and the collection of evidence, the investigating agent(s) should search for suicide notes and personal writings (such as diaries, journals, letters, poems, etc.) which may indicate a proclivity towards suicide. If the victim had access to a personal computer or work computer, cellular phones, PDA (also known as palm pilot), etc., appropriate steps should be conducted to seize any electronic media for further examination.

b. Interviews. Inquiries should include interview of all acquaintances, military associates, relatives, and neighbors who may be able to provide information concerning the deceased's personality, habits, and activities. In particular the following considerations should be covered and documented:

(1) Recent change in personality of the deceased,

(2) Dissatisfaction with employment or military assignment,

(3) Evidence of anxiety or depression,

(4) Indication of alcohol/drug abuse,

(5) Marital discord,

(6) Financial problems,

(7) Failing health or imagined failing health,

(8) Unwise or indiscreet emotional/sexual involvement with members of the opposite or same sex,

(9) Indication of indiscreet safeguarding or handling of classified material, and

(10) Previous attempts or utterance of intent to commit suicide.

30-13.6. Where suicide notes or other writings indicative of suicide are discovered, those documents should be forwarded for laboratory examination requesting fingerprint identification and to authenticate the authoring by the deceased. Obtaining the deceased's military or employment record to ensure an adequate sampling of the deceased's known handwriting may also be necessary.

30-13.7. Firearms Related Suicides. When an apparent suicide resulted from a gunshot wound, investigation must establish the deceased's normal "strong hand." Interpretation of wounds by the pathologist may establish which hand was used to inflict the injury. However, where interpretation of the wound determines that it was not inflicted with the deceased's "strong hand," suicide cannot be ruled out. Some suicide victims may use the "weak hand" and the investigating agent may encounter cases where the deceased used his toes or feet to discharge the firearm. In cases where firearms are used, the deceased's hands must be processed to detect the presence of gunshot residue (GSR). The victim's hands should be protected with paper bags at the scene and GSR samplings done at the autopsy prior to fingerprinting the victim. This procedure can be accomplished at the scene prior to transporting. In any case, it is highly recommended that the servicing forensic consultant be contacted prior to administering a GSR test. It must be ensured that anyone reporting the witnessing of the suicide is also tested for GSR. The firearm and any expended bullets or cartridge cases recovered at the scene and bullets recovered from the victim's body at autopsy must be submitted for laboratory examination and comparison. In all cases involving firearms, the firearms should be submitted to a laboratory for fingerprint processing and technical examination to establish the pounds of trigger pull required to activate the weapon and to determine if the weapon was in proper working condition, and ballistics testing as needed.

30-14. HOMICIDE VERSUS SUICIDE OR ACCIDENTAL DEATH. The question of homicide, suicide, or accidental death often confronts the investigating agent. The following are basic considerations that an agent must be aware of when investigating a death in which the manner is not readily apparent.

a. Shootings. Evaluation of the distance of the weapon to the deceased is paramount. To establish suicide, the shot must have been fired within a distance physically allowable by assessing the length of the deceased's arms and the weapon used (unless a mechanical contraption was used to fire the weapon). Most suicide victims hold the firearm against the skin or at a close distance. All or most of the discharge residue should have been blown into the wound cavity and readily recognized at autopsy. However, gunpowder may not be found in a gunshot wound to the heart, due to the blood flow carrying the gunpowder away from the wound. Presence of widespread "tattooing" is suggestive of a shot fired at some distance. The firearm should have been held or fired with the deceased's "strong hand," however the use of the "weak hand" does not rule out suicide. Multiple wounds (including wounds to the head) may be encountered in suicide cases. Multiple shots are generally in the same area of the body. It is unusual to find wounds scattered over different portions of the deceased's anatomy. Under such circumstances, homicide should be considered. "Test shots" fired into walls, floors, ceilings, and furniture is also common in suicide cases. The victim may fire several shots prior to inflicting the lethal wound to test the noise and recoil of the firearm or to muster the courage to complete the act. Contact shots may be muffled

and inaudible to individuals nearby. Gunshot residue is sometimes present on the deceased's hand(s). With rifles and shotguns in good working condition, it is very unlikely that identifiable GSR will be found on the hand that pulled the trigger. Different firearms tend to deposit GSR in different patterns and this may be useful in determining whether a bullet wound was self-inflicted. Occasionally, GSR deposits are noted on both hands, especially on the one that was used to steady the weapon while the other pulled/pushed the trigger. Hands suspected of having fired a gun should never be fingerprinted until after proper GSR swabbings have been collected. Absence of gunshot residue does not rule out suicide or imply the gun was fired by another person, as some modern ammunition does not contain antimony and barium as primer components, and many factors are involved in the deposition of GSR on the hands of shooters. (b)(7)(E)

(b)(7)(E)

b. Incised and Stab Wounds. Evaluation of the location, pattern, and age of incised wounds and stab wounds is essential. Incised wounds in various stages of healing may be encountered and indicate previous acts of attempted suicide. Self-inflicted stab wounds are encountered in suicide investigations although they are somewhat rare.

c. Death Involving Asphyxiation. Guidance for investigation of deaths associated with asphyxiation was presented earlier in this chapter. However, the investigating agent should consider the following during the investigation. Death by hanging is commonly associated with suicide. Hanging may occur in any position that allows arresting of the arterial blood supply to the brain or obstruction of the airways. While homicidal hanging is rare, the death scene and condition of the deceased's body must be consistent with self-administered hanging. Postmortem lividity should be present in the lower extremities and the groove or furrow around the neck should follow the jaw line and form the apex at the position of the knot. It is impossible for an individual to commit suicide by manual strangulation unless a mechanical contraption is used. Fracture of the hyoid bone is frequently associated with manual strangulation. (b)(7)(E)

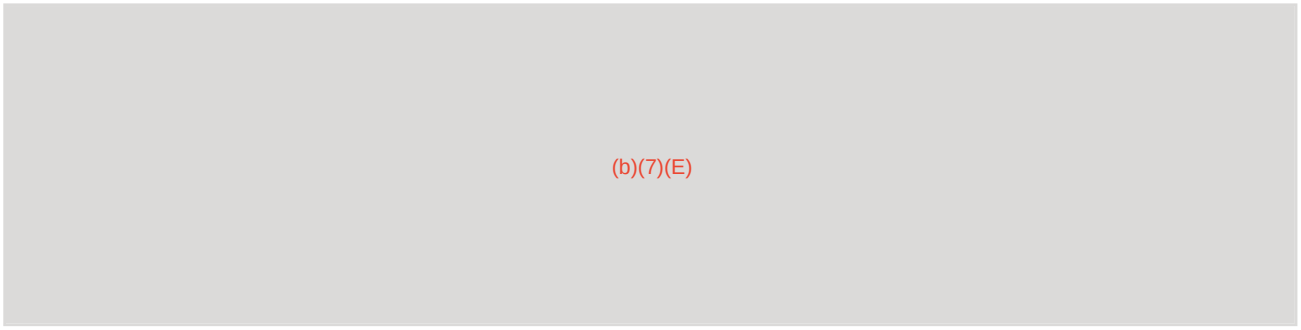
(b)(7)(E)

(b)(7)(E) In such cases, it is possible that the deceased hanged oneself and was later moved by friends or relatives to cover the act of suicide. This often occurs to allow relatives to collect insurance benefits or to avoid the stigma attached to suicide.

(b)(7)(E)

(2) Carbon monoxide poisoning, previously discussed in this chapter, is also a common and often encountered method of suicide. The death scene and postmortem changes on the deceased's body must be carefully considered. Postmortem lividity must be consistent with the position of the

body. An autopsy is essential to determine the presence of carbon monoxide in the deceased's remains.



(4) Jumping/Falling Deaths. Jumping from a height is a common method of suicide. Inspection of the death scene, particularly the point at which the deceased jumped or fell, is essential. Indications of a struggle at the location may be indicative that the victim was pushed or accidentally fell during a struggle. Measurements of distance from the point of the jump/fall and the point of impact should be recorded in the death scene Investigative Action (IA). Note that the interview of witnesses at the scene is often the key investigative component in determining the manner of death in jumping or falling deaths.

30-15. VEHICULAR DEATHS. All vehicular deaths, whether the victim was the driver, passenger, pedestrian, or a combination thereof, will be investigated under the Case Category7H.

30-15.1. When NCIS receives a request for investigative assistance from a non-DoD agency regarding a vehicular death or receives a request from a command for the details and disposition of a vehicular death, the NCIS investigative case category is Category 7H, with the appropriate narrative description of reciprocal or details and disposition. When command requests details and disposition, a copy of the investigative report shall be requested from the appropriate investigative agency. If authorized by that agency, a copy of their investigative report will be appended as an exhibit and disseminated to the command. If authority to release is not obtained, a review of the report will be made an exhibit and the police report will be maintained in the file until destroyed locally.

30-15.2. When NCIS has primary or joint investigative jurisdiction of a vehicular death, the NCIS investigation may not be closed without the death scene being conducted, and the autopsy report, toxicology report, and death certificate being obtained. If an autopsy is not authorized or conducted, a death certificate must be obtained. The vehicle death investigation shall be presented to the Field Office Death Review Panel (DRP), for authority to close the investigation (except for suicide by vehicle). The death scene examination conducted on a vehicular death should be coordinated with a trained accident investigator and/or accident reconstruction specialist when available. Access to personnel possessing specialized training may be obtained through the command, local law enforcement agencies, or NCISHQ.

30-15.3. A vehicular accident, resulting in non life-threatening injury, and in which the vehicle operator departed the scene without rendering assistance or making identity known, shall be investigated under Case Category 7T (Traffic Accident) per NCIS-3 Chapter 33. A vehicular

accident that results in personal or government property damage wherein the vehicle operator flees the scene is also to be investigated under Case Category7T.

30-16. IDENTIFICATION OF UNKNOWN REMAINS

30-16.1. The identification of unknown remains is needed in all cases for the following reasons: (1) completion of official records, (2) notification of next of kin, (3) settlement of military survivor's benefits, estates, and insurance claims, and (4) establishment of the corpus delicti of homicide.

30-16.2. The investigating agent may be tasked with conducting an inquiry regarding the discovery of a body, which in various stages of decomposition ranges from an intact body to a few pieces of skeletal remains. The body may have also been badly incinerated by intense burning. These investigations call for close coordination between the investigating agent, servicing forensic consultant, and the pathologist, and may eventually require the assistance of other experts representing several components of the forensic investigative community, including: (1) fingerprint expert, (2) forensic anthropologist, (3) forensic odontologist (dentist), (4) radiologist, and/or (5) forensic serologist/DNA expert.

30-16.3. Where only a few bones are recovered, the first essential task is to determine if the skeletal remains are of human origin.

30-16.4. Identification Procedures. Identification is based on comparison of known information derived from examination of the remains by a forensic expert(s) with known information derived from various sources, including official records and witness interviews. A coordinated examination of the body/remains by the investigating agent and pathologist should include documentation of all observations possible based on the condition of the body. The following should be accomplished when possible:

a. Photography of the Body/Remains. Where possible the photography should depict full face and profile of the body. All scars, marks, and tattoos should be photographed.

b. All clothing, jewelry, and items of identification associated with the body should be recorded and photographed.

c. The clothing, wallet, and other personal items should be inspected for presence of identification documents.

d. All keys associated with the body should be retained as they may later provide access to living quarters, automobiles, or other secured property owned by the deceased.

e. The fingerprints, palm prints, and footprints should be recorded.

f. Samples of head and pubic hair and blood (using a purple top tube containing the preservative EDTA) should be obtained.

g. Full body X-rays, as well as those of skeletal remains should be taken.

h. Dental X-rays and a complete chart should be made of the deceased.

i. Any eyeglasses or contact lenses associated with the body should be retained as evidence. The prescription of eyeglasses and contact lenses can be determined and compared with record entries. Manufacturer's data is inscribed on some contact lenses and visible when viewed under ultraviolet light.

j. All clothing should be inspected for the presence of laundry marks.

k. All dentures, bridgework and other dental devices should be retained and inspected by a forensic odontologist. Some military departments, prison/correctional facilities, and other public agencies mark dentures and dental bridgework for identification.

NOTE: Caution is to be exercised when attempting to effect identification based on the clothing and personal effects found on the body. Likewise, identification of badly injured or decomposed bodies by friends and relatives is not recommended.

30-16.5. Record Information Sources. The following records may be useful for comparison with the results of autopsy and other investigative findings:

a. Missing persons reports,

b. Fingerprint records,

c. Dental records-including denture identification records,

d. Health records to include determination of the blood type and any history of injury to bones or surgical removal of organs,

e. Antemortem X-rays,

f. Employment/military records,

g. Police reports, and

h. Eye glasses/contact lens prescription records.

30-16.6. In cases where the preliminary investigation does not identify the body or remains, the following information may be derived from an examination by the pathologist or other forensic expert (such as the forensic anthropologist):

a. Race, sex, and estimated age of the deceased;

b. Estimated time of death or duration of time between death and discovery of the remains;

c. Possible occupation of the deceased;

d. If the remains are of a female, determination may be made that the individual has borne a child; and

e. The height, weight, and general stature of the deceased can be estimated.

30-16.7. Where decomposed or skeletal remains are discovered outdoors, the investigating agent should consider special death scene examination techniques. Once the remains have been removed, the earth in the area in which the body was discovered should be sifted to a depth of approximately 12 inches beneath the surface. Sifting of the soil may assist in the recovery of expended bullets, broken knife blades, items of jewelry, teeth, and other items of evidence which may have fallen from the body and become embedded in the soil. In cases where it appears a portion of the skeletal remains is missing, the investigative scene should be expanded to determine if animals carried parts of the body/skeleton away.

30-17. INDEXING OF UNIDENTIFIED REMAINS

30-17.1. Due to the manner in which data is stored in the NCISHQ Case Information System (CIS), the following procedures should be utilized for titling unidentified human remains. The pseudonyms of Doe, John; Doe, Jane; or Doe, Unknown; followed by NMN (no middle name), will be entered as a victim title. The Personal Title Status Entry will be UNK (unknown). Sex and race codes will be entered, or in the case of skeletons, the best that can be determined. "N" will be used for the Security Clearance Code, and "ZZZZ" will be used as the Status Identifier Code, unless the accurate information is available. For example:

V/DOE, JOHN (NMN)/UNK
M/U/ZZZZ/N///

V/DOE, JANE (NMN)/UNK
F/U/ZZZZ/N///

V/DOE, UNKNOWN
Z/U/ZZZZ/N///

30-17.2. This practice will allow the report to be indexed so that the case file may be retrieved at NCISHQ. Files will not be indexed into the Defense Clearance and Investigations Index (DCII), rather the files will be assigned a NCIS Dossier with the number being manually entered into the NCISHQ CIS. John and Jane Doe listings in the title block will be used only for the purpose of tracking and titling unidentified human remains.

30-17.3. Cases involving John or Jane Does can be transferred at any time to the Cold Case Squad at the discretion of the field office SAC. It is important to document in the ROI a Medical Examiner number or other means to permit tracking the location where the remains are buried or stored.

30-17.3. Original Victim Fingerprint Cards

a. Original victim fingerprint cards are NOT to be retained in the closed case file and will be handled based in the following manner:

(1) Original identified victim fingerprint cards will be destroyed upon official closing of the case/investigation.

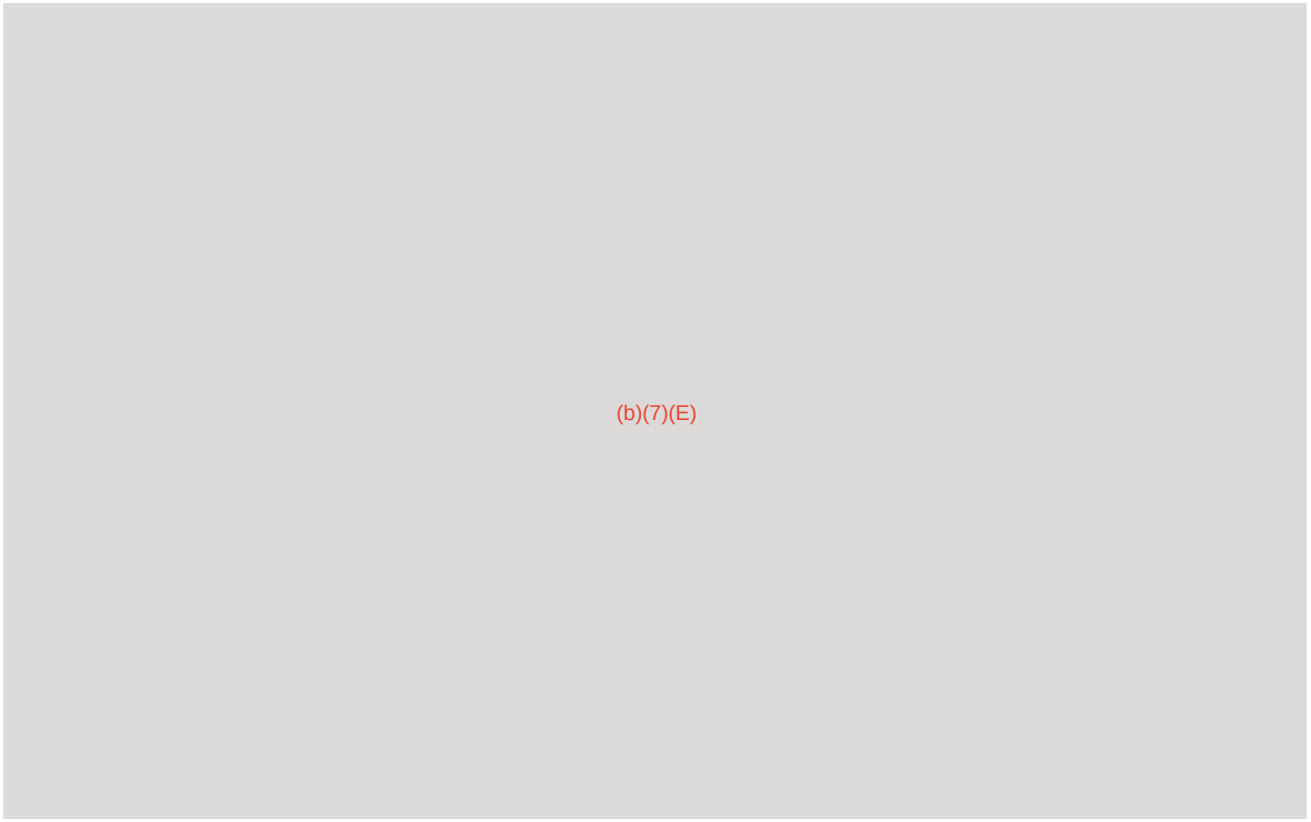
(2) Original unidentified victim fingerprint cards will be sent to the FBI Missing Persons Section. The only exception to this will be unidentified victims suspected of being non-U.S. persons. In these cases, please contact NCIS, Code 24B3 for guidance.

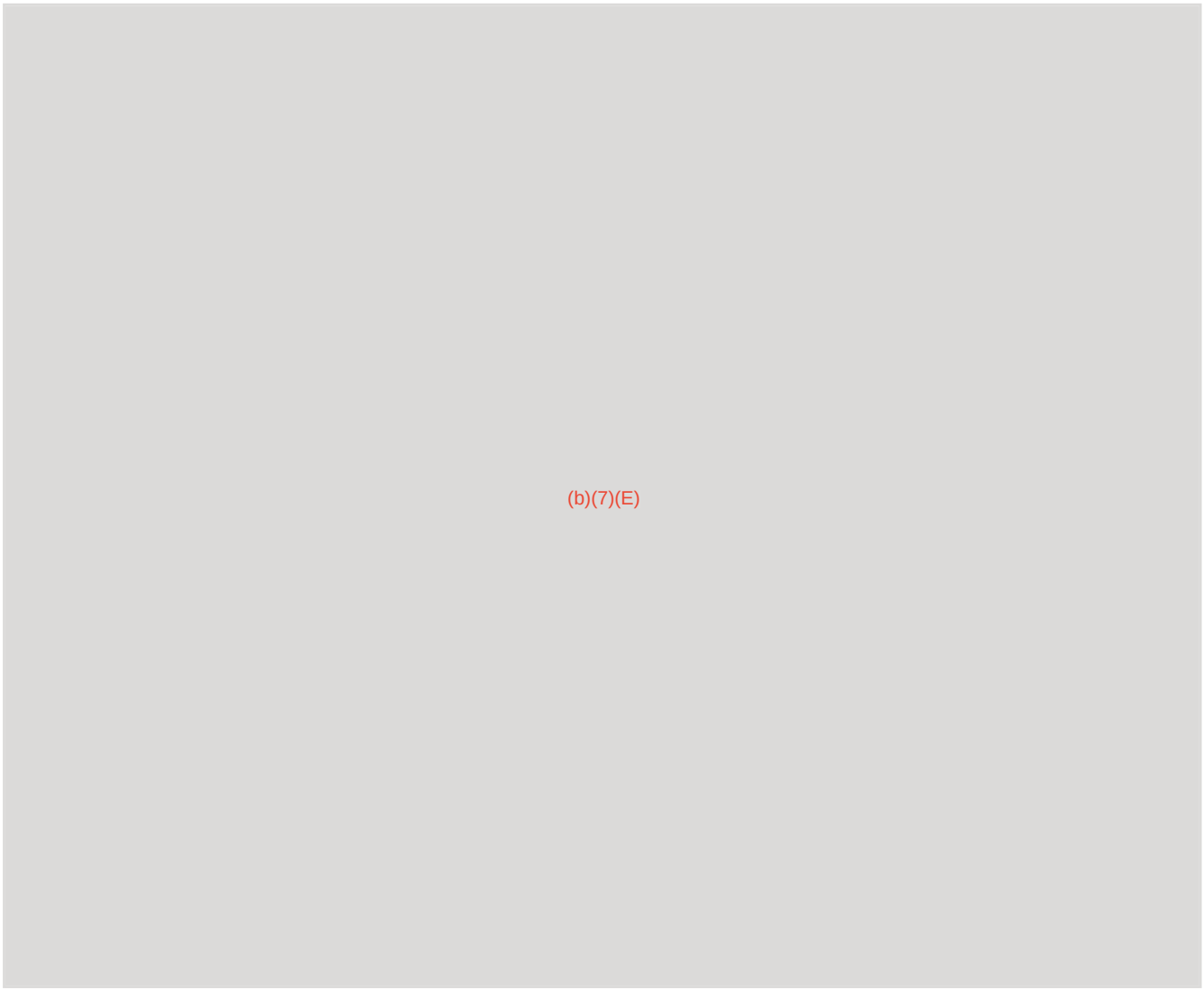
b. A copy of the victim fingerprint cards should be placed in the case file if they are listed as an exhibit, enclosure, or attachment to a ROI.

c. Submit the original unidentified/unknown victim fingerprint cards to the FBI Missing Persons Section, address below. Include a NCIS cover letter containing the submitter's name, contact information, NCIS case control number, and direction to have the results of any search reported back to the submitting agent. Mail the cover letter and original fingerprints to:

DOCSPE
1000 CUSTER HOLLOW ROAD
CLARKSBURG, WV 26302-9924

For further guidance, contact NCIS Code 24B3.





30-19. ARMED FORCES MEDICAL EXAMINER SYSTEM (AFME)

30-19.1. The AFME System is administered by the Armed Forces Institute of Pathology (AFIP), Washington, D.C. The AFME System is staffed with board-certified forensic pathologists trained to conduct autopsies and apply medicolegal training to investigations and judicial proceedings. It is therefore essential that in all death investigations wherein NCIS retains primary investigative jurisdiction, the Regional AFME be expeditiously (within 24 hours) notified by the NCIS field office of the initiation of the investigation. In the event notification of an AFME cannot be made, NCISHQ, Code 23B should be immediately apprised so that appropriate personnel at the AFIP can be contacted. After normal business hours, apprisal of Code 23B personnel can be made through the Law Enforcement Desk of the NCISHQ Multiple Threat Alert Center (MTAC).

30-19.2. In situations where another jurisdiction has assumed responsibility to conduct the autopsy (such as overseas), the Regional AFME's assistance should still be sought, at minimum to act as an observer with the concurrence of the local government. See Appendix (5) for locations and phone numbers.

30-20. PSYCHOLOGICAL AUTOPSY AND PSYCHOLOGICAL REVIEW

30-20.1. Psychological Autopsy. The investigation of equivocal deaths frequently requires the consultation with a mental health professional trained or credentialed in forensic psychology (or psychiatry). Many operational psychologists are experienced in forensic matters and criminal investigations and can render valuable assistance in equivocal/unexplained death investigations. The psychological autopsy is a postmortem investigative tool that assists the medical examiner, not NCIS case agents, in understanding the circumstances leading up to the death and the decedent's role in his/her death. NCIS case agents considering psychological consultation services for an investigation should see the section on Psychological Reviews below.

a. A psychological autopsy is a detailed written report prepared by a forensic psychologist for the sole purpose of assisting the attending medical examiner when the manner of death is uncertain (i.e., suicide vs. homicide vs. accident). It is an investigative tool that reconstructs the decedent's background, personal relationships, habits, character traits, life stressors, coping patterns, mental health, and behaviors preceding the death. Its purpose is to contribute to an understanding of the relationship between the decedent's personal history, life stressors, behaviors, and his/her death.

b. Traditionally, requests for psychological autopsies on NCIS investigations were submitted by the Regional AFMEs to the NCIS Psychological Services Unit (NCISHQ Code 02D) via the AFIP. However, the AFIP recently assigned its own forensic psychiatrist to conduct all AFIP psychological autopsies. Currently, AFME requests for psychological autopsies are handled within AFIP channels. Should a Regional AFME request a psychological autopsy through the NCIS case agent, the case agent should forward the request to the NCIS special agent assigned to AFIP, who will then forward the request to the AFIP forensic psychiatrist/ psychologist. If the AFIP forensic psychiatrist/psychologist is unable to fulfill the request, the NCIS special agent at AFIP should forward the request by phone call or email to the NCISHQ Code 23B 7H desk officer, who will then forward it to the NCIS Psychological Services Unit.

c. Municipal, county, and state medical examiners may be aware that psychological autopsies are conducted by the NCIS Psychological Services Unit and may initiate a request for this service. In this situation, the NCIS case agent should submit the request by phone call or email to the NCISHQ Code 23B 7H desk officer, who will then forward it to the NCIS Psychological Services Unit. Do not send a lead.

d. If the AFIP forensic psychiatrist/psychologist is unable to conduct the psychological autopsy, it will be completed by the NCIS Psychological Services Unit. In this scenario, the NCIS special agent at AFIP should forward the request by phone call or email to the NCISHQ Code 23B 7H desk officer, who will then forward it to the NCIS Psychological Services Unit. Following receipt of request, the psychological autopsy investigative outline will be sent to the case agent. This document provides the case agent guidance in collecting pertinent information for the psychological autopsy. Relatives, friends, and co-workers of the deceased should be interviewed with the aim of documenting personality characteristics, personal habits, work performance, lifestyle factors, stressors, and other factors (see Appendix (6)). Written materials

of the deceased such as diaries/journals/personal writings, computer files, letters, notes, poetry, appointment schedule, etc., should also be collected. Additionally, attention to personal effects such as magazines, videos, and photographs should also be noted and collected. A review of the service record, medical record, and other available records (e.g., Family Service, brig records) should be conducted. The NCIS Staff Psychologist will review the complete investigative file and author a report. Upon completion, the report will be forwarded by the Staff Psychologist directly to the requesting medical examiner and provide a copy to the case agent. The report is not attached to the NCIS investigative file, but may be retained with the agent's case notes. The only exception is when the medical examiner appends the psychological autopsy to the final autopsy report. In those instances, the psychological autopsy should remain appended to the autopsy report.

30-20.2. Psychological Review. The psychological review is the NCIS case agent's psychological tool for death investigations. Like the psychological autopsy, the psychological review is a reconstructive study of the decedent's life, personality, relationships, behavior, and psychological functioning to understand the circumstances of the events that preceded the death. However, it is a less intensive process than the psychological autopsy and it provides a psychological consultation to the case agent instead of to the medical examiner. The psychological review can be used by the case agent to investigate issues related to the manner of death (e.g., assess risk factors for suicide, motivations for homicide, or behaviors indicative of an accident). The psychological review may provide the case agent with further behavioral investigative leads, refined questions for collateral interviews, or strategies for suspect interrogations.

a. The NCIS case agent should submit their request for a psychological review by phone call or email to the NCISHQ Code 23B 7H desk officer, who will then forward it to the NCIS Psychological Services Unit. Do not send a lead. The consultation will follow the same investigative protocol as used with psychological autopsies. Requests for psychological reviews can be submitted at any time during the investigation, but are often most beneficial to the case agent if submitted at the opening of the investigation. When submitted at opening, the psychological review can assist the case agent with prioritizing leads, strategizing interviews, and focusing investigative resources. This consultation is ongoing and continuous; as the investigation proceeds, results should be continuously forwarded to the NCISHQ Code 23B 7H desk officer, who will provide the information to the NCIS Staff Psychologist. The NCIS Staff Psychologist will review the information and provide ongoing consultation results to the case agent via phone call, email, VTC, or site visit consultation. If warranted, the NCIS Staff Psychologist will author a memo or report. All written products (e.g. emails, memos, or reports) should be retained with the agent's case notes and not attached to the investigative file. Any reference to the psychological consultation in the formal investigative paper (i.e. ROI or IA) should first be discussed with the Staff Psychologist.

b. For cases in which a suspect has not yet been identified, the case agent should consider requesting a psychological review. The NCIS Staff Psychologist will conduct the consultation in partnership with an NCIS expert in death investigations (e.g., an NCIS Forensic Consultant or Homicide Analyst). The case agent will be provided with a behavioral and forensic assessment of the death scene, and personality/behavioral characteristics of the suspect.

c. If a case agent has any questions as to whether a psychological review or psychological consultation is appropriate, contact (via phone or email) the NCIS Psychological Services Unit at NCISHQ Code 02D.

30-21. REPORTING REQUIREMENTS

30-21.1. Detailed and timely reporting is mandatory in all death investigations. As case category 7H includes all manners of death, the category entry at the top of all SSDs should always read "DEATH." Entries of "HOMICIDE" or "SUICIDE" are incorrect, as there are currently no separate case categories for those manners of death. An investigation involving the death of a person, even an apparent suicide, should list the deceased as a victim. ROI (CLOSED) or ROI (INFO) will not be used to document a death investigation. The only exceptions to this policy are the investigations with a command line of NON-DoD INTEREST, which may be reported by ROI (CLOSED), and cases that are initially responded to, documented, and then determined to be medically attended deaths. The ROI (OPEN) will specifically state why NCIS is conducting the investigation (e.g., at the request of the command, to obtain details and disposition, due to NCIS having primary jurisdiction). The ROI providing the final autopsy report and/or the death certificate will document the results of the autopsy, including both the cause and manner of death, as determined by the pathologist, coroner, etc. In the event a Report of Casualty (DD Form 1300) is submitted, the ROI will document the cause and/or manner of death indicated on the report. In the event the victim's body is not recovered, ensure that a DD Form 1300 is obtained. If the victim's body is not recovered at the time of the ROI (CLOSED), a NCIC missing persons report must be made. The NCIC missing persons entry will assist in identification of the remains if they are later found. When sending the ACTION for the missing persons entry, the ROI Action should continue to be electronically addressed to Report Writing Electrical Destination "/NN/" with the ACTION entry section addressed to 00NN.

30-21.2. To ensure that NCIS death investigations are completely objective, "Statutes" paragraphs will not be included in any death investigative reports until such time as evidence surfaces to indicate homicide as the manner of death. Once homicide has been identified as the manner of death, the appropriate criminal statute(s) will be cited.

30-21.3. Death investigations within the category to be reviewed by the NCISHQ Death Review Board (DRB) (section 30-27 pertains), whether conducted jointly with another agency or solely by NCIS, will adhere to 30-day reporting requirement. These special reporting requirements for death investigations apply only to investigations that are being actively and fully pursued by NCIS (e.g., NCIS controlled cases and joint cases as opposed to those cases initiated solely as reciprocal, details and disposition, or specific phase cases where NCIS is minimally assisting another agency). As required by NCIS–1, Chapter 25, investigations with Director's Special Interest (DSI) or Special Interest (SI) designation mandate initial report documentation at the end of the first 30-day period with a ROI (INTERIM) to include copies of all exhibits and thereafter a 30-day ROI reporting requirement assuming the investigation is not yet complete. Death investigations not within the category to be reviewed by the DRB, Adult Natural and Accidentals, will follow standard 60-day reporting. Exhibits will include all available supporting documentation pertaining to leads completed up to that point and will be sent to NCISHQ, Code 23B. All major inconsistencies

(between witnesses, physical evidence, etc.) should be addressed and reported by ROI. When substantial participation or investigative assistance is provided to a non-DoD agency, these investigations will be thoroughly documented as if NCIS had primary jurisdiction. Upon approval/authorization from the Death Review Panel (DRP)/DRB to close an investigation the case control office will submit a ROI (CLOSED).

30-21.4. The examination of the death scene is one of the most important elements of any death investigation, even if the body has been removed prior to NCIS arrival. This examination shall be conducted professionally in a timely manner and fully documented by an Investigative Action (IA). It will be labeled "Death Scene Examination," not "Crime Scene Examination," as often there is no actual crime involved with a death. Labeling this IA as a crime scene examination in cases of suicide and accidents fosters later confusion when the report is read by persons unfamiliar with the investigative process. The IA will contain the complete results of examination, sketch/drawings including measurements, evidence seized, and other items listed in NCIS-3, Chapter 12. Signs of foul play, or the lack thereof, should specifically be documented in the IA. Enclosures to the death scene IA will include, at a minimum, the completed sketch (not a rough draft) and color photographs (developed photographs and not negatives, instant Polaroid photos, or proof sheet). NCIS-3, Chapter 11, states a photographic log will be prepared in the form of an IA describing to the reader what each photograph/negative depicts. This terminology is confusing since a true photo log is prepared at the scene to document details of each exposure taken. It contains information about the type of camera and flash used, as well as the F-stop, exposure time and film speed for each exposure taken. As with the negatives, the photo log should be kept with the case agent's notes and used if needed to support the agent's testimony at trial. Due to myriad legitimate reasons (bracketing, duplicate shots, focusing issues, etc.) seldom are all of the shots actually taken at the scene submitted in the investigative report. Submitting a complete photographic log with only selected prints attached confuses readers, specifically those who obtain our reports via the Freedom of Information Act (FOIA). Each attached photograph will be individually identified by letters and will be individually described in the Death Scene or Photographic Coverage IA. One copy of the ROI (INTERIM) with the color photographs and all other listed exhibits will be mailed to Code 23B when the ROI (INTERIM) is transmitted to NCISHQ. Death scenes located in a room(s) of a building should show a complete panoramic view of the room(s). Additional guidance concerning photography in death cases is provided in following sub-sections. Any forensic analysis on items seized from the scene can be documented by separate laboratory report when received. If a videotape is made of the death scene, the video will be treated the same as photographs taken. Therefore, the videotape will be submitted as an enclosure or exhibit to the death scene IA and will not be placed into evidence. Code 23B will only need one copy of the videotape. Additionally, 911 recordings that are obtained during the investigation must be transcribed and documented via an IA. The 911 recording will be provided as an enclosure to the IA.

30-21.5. The text of the pertinent ROI (INTERIM) or ROI (CLOSED) will document the results of the autopsy, including both the cause and manner of death, as determined by the pathologist, and will clearly state that the pathologist made the determinations (NCIS does not make such determinations). An example would be "the King County Medical Examiner determined the cause of V/SMITH's death as a gun shot wound to the head and the manner of death as Suicide."

30-21.6. IAs reporting death investigations should report all investigative steps conducted, not just those that appear fruitful. NCIS is routinely questioned by outside sources with regard to the logic behind investigative steps. While steps are generally accomplished, they are not documented on occasion because the results were considered unproductive. It is imperative to document ALL investigative efforts in death cases.

30-21.7. One copy of all ROI (INTERIM)s shall be submitted to NCISHQ documenting NCIS control and joint investigations, including color photographs and all other listed exhibits, enclosures and/or attachments. This does not apply to reciprocal, specific phase and/or details and disposition cases. This copy is provided to NCISHQ during the pendency of the case, as the ROI (INTERIM)s are generated. Only one copy of videotapes or audiocassettes is required in Code 23B; therefore, copies sent with the ROI (INTERIM) while cases are pending are sufficient. The complete original file is provided to NCISHQ upon case closure. Closed control and joint death investigations are routinely provided to the AFIP for review, as required by DoD instruction. True digital photos produced directly from a high quality 35mm digital camera are authorized and can be used by offices that are not serviced by photo centers with traditional 35mm wet film development capabilities. Black and white photocopies of photographs (e.g. xerox copies), proof sheets alone, or instant Polaroid photographs are not acceptable as exhibits. Photographic negatives and proof sheets will be retained with case notes and not submitted to NCISHQ as exhibits. Black and white photocopies of photographs of death scenes and autopsies in 7H cases are unacceptable. Electronic media (e.g., computer disks, CDs, DVD, digital media sticks) may be included in the case file. Please refer to NCIS-1, Chapter 25, Section 24. for additional guidance. Field offices will retain case notes until files are purged following completion of all appeals and other reasons for retention have expired. It should be noted that case notes are subject to FOIA release until destroyed and will not be submitted as part of the original case file unless specifically requested by Code 23B.

30-21.8. In investigations involving U.S. Navy and Marine Corps personnel as victims or suspects, the "final" report of autopsy (including the toxicology report) and Death Certificate must be obtained and made a part of the investigative dossier prior to closing the investigation, as stated above. All Case Category 7H investigations in which the autopsy report is in a foreign language must have the full autopsy report translated into English. A condensed English language version of a foreign language autopsy is not acceptable for NCISHQ or AFIP purposes.

30-21.9. In reciprocal investigations conducted for other law enforcement agencies where there is any DON interest (e.g., military suspect/victim or crime aboard a military installation), a copy of the requesting agency's death investigation will be obtained, however the report will not be made a part of the NCIS ROI unless needed by command for prosecutive purposes. Otherwise, the information contained in any police report will be paraphrased in an IA. The police report will be maintained in the case agent notes and destroyed with the file at the appropriate time. A police report will be made part of the ROI only when needed by command for prosecutive purposes.

30-21.10. In cases where a death has been ruled a homicide or when the manner of death is surrounded by unclear circumstances, logical leads will be pursued until a suspect is apprehended, or further forensic testing changes the manner of death to accidental, natural, or suicide. “Undetermined” is a valid manner of death when the medical examiner cannot make a definitive ruling.

30-21.11. The Under Secretary of Defense Memorandum/Notification of Department of Defense-Related Fatalities Due to Domestic Violence or Child Abuse/04MAR05 directs each service Secretary to ensure a multi-disciplinary, impartial review is conducted of each DoD related fatality known or suspected to have resulted from domestic violence or child abuse. Specifically, incidents involving: (1) a member of a military department on active duty; (2) a current or former dependent of a member of a military department on active duty; or (3) a current or former intimate partner who has a child in common and/or has shared a common domicile with a member of a military department on active duty.

a. Fatality reviews are deliberate examinations conducted only after all related law enforcement investigations, autopsies, and court trials have been concluded. The team, which comprises NCIS, Family Advocacy, JAG, Armed Forces Center for Child Protection, Domestic Violence Analyst Command, and physicians from the National Naval Medical Center, Bethesda, MD, meets in closed session to review all related documentation for the purpose of formulating lessons learned and identifying patterns and trends.

b. The fatality review team will generate an annual report to the Office of the Deputy Under Secretary of Defense for Military Community and Family Policy. The report shall include: (1) data setting forth victim demographics, injuries, autopsy findings, homicide or suicide methodologies, weapons used, police information, assailant demographics, and household/family information; (2) legal dispositions of the investigation; (3) intervention efforts and failures of the Family Advocacy Program, Child Protective Services and law enforcement; (4) a discussion of significant findings; and (5) recommendations for systemic changes.

c. Each military department fatality review team will comply with the requirements of the DoD Privacy Program, and any state law that protects the confidentiality of the identities of those involved. Internal team documentation will be protected under the DoD FOIA Program or under any relevant state law.

d. Within 72 hours of NCIS initiating an investigation which meets the criteria as stated above, the case information shall be reported via the DON Child Abuse and Domestic Violence Fatality Initial Notification (DD Form 2901). The DD Form 2901, which has been linked to the NCISnet, can be accessed by going to "Downloads-> Forms-> Investigative Forms" and is listed as "Child Abuse and Domestic Violence Fatality Initial Notification (DD Form 2901)".

e. Once completed, this form will be saved and emailed to Code 23B for inclusion in the fatality review team database. If Internet access is not available to obtain the DD Form 2901, please contact Code 23B to obtain a form.

30-22. FAMILY LIAISON PROGRAM. The NCIS Family Liaison Program was established to provide timely, accurate, and consistent information throughout an investigation when communicating with the next of kin (NOK) of military victims when NCIS has primary investigative jurisdiction in a non-homicide death investigation. The following concepts have been established to define the Family Liaison Program.

30-22.1. The NCIS Family Liaison Program establishes direct communication between NCIS and the primary/secondary NOK of a deceased military victim of a NCIS death investigation. NOK may include, but is not necessarily limited to: spouse, parents, siblings, children, and guardian of the victim. Primary next of kin (PNOK) is determined by the designation as primary beneficiary in the victim's service record book. The Family Liaison Coordinator establishes contact and addresses NOK concerns regarding the NCIS investigation. The Family Liaison Coordinator provides releasable investigative information to the NOK throughout the course of the investigation, and close communication often continues after the investigation is closed. Family liaison is usually provided when a military victim dies from an apparent self-inflicted injury, an accident, or when the cause and manner of death is undetermined.

30-22.2. Family liaison is not provided when the manner of death is homicide, medically determined to be from natural causes, or traffic accidents. Additionally, family liaison is not provided on reciprocal investigations when NCIS does retain primary investigative jurisdiction. Questions concerning these reciprocal death investigations should be referred to the law enforcement agency that retains primary jurisdiction. Family liaison may be provided when the death occurs outside the United States and the NOK experience difficulty communicating with the foreign law enforcement agency that retains jurisdiction. Family liaison is not provided on missing person investigations unless there is credible evidence that the victim is deceased and the case category will be changed to 7H. Family liaison will not be provided when the cause of death results from combat operations in a hostile/combat environment as designated by the DoD. Designated NCIS regional Victim/Witness Coordinators are encouraged to assume active and aggressive family liaison services during investigations where the NCISHQ Family Liaison Coordinator does not assume these responsibilities. These restrictions are guidelines and not necessarily inclusive. Case agents are encouraged to contact the Family Liaison Coordinator when questions arise concerning family liaison services and prior to offering NCISHQ family liaison services to the NOK.

30-22.3. The decision to conduct family liaison with the NOK will be made by NCISHQ, Code 23B and the NCISHQ Family Liaison Coordinator. The NCISHQ Family Liaison Coordinator will be the primary point of contact for the NOK concerning investigative issues. This does not preclude contact between the case agent and the NOK. However, all NOK contact, to include the coordination of interviews of NOK, should be coordinated through the NCISHQ Family Liaison Coordinator.

30-22.4. The Family Liaison Coordinator confers with the case agent, the NCISHQ 7H (desk officer) case reviewer, and the U.S. Navy or USMC Casualty Assistance Calls Officer (CACO), at the onset of the investigation to ascertain investigative facts and family concerns. The Family Liaison Coordinator also confers with the NCISHQ FOIA Coordinator before providing releasable investigative information to the NOK.

30-22.5. The mission of the NCIS Family Liaison Program is to communicate contents of releasable information concerning NCIS death investigations to the NOK in a timely and consistent manner. The Family Liaison Coordinator informs the NOK on NCIS policy and procedures, reasons for the conduction of an investigation, and procedures in the investigative process (including the NCISHQ DRB and FOIA procedures). The Family Liaison Coordinator also may act as an information conduit between the CACO, the victim's command, and the NOK for issues not

the responsibility of NCIS but of NOK concern.

30-22.6. A toll free number (1-800-479-9685) has been installed at NCISHQ, Code 23B, and will be monitored during normal business hours by the Family Liaison Coordinator. The Family Liaison Coordinator will provide the number to NOK during initial contact. Agents are advised not to provide the number to NOK without prior coordination with the Family Liaison Coordinator. For callers from outside the United States, use DSN: 288-9224 and commercial (202) 433-9224 to make contact with the Family Liaison Coordinator. Numbers are restricted for family liaison purposes only.

30-22.7. In almost all cases, the NOK will request a copy of the NCIS investigation through FOIA. Redacted copies of all reports, to include exhibits, will be provided to the NOK after the investigation is closed and the request processed through FOIA. These reports will be closely scrutinized by the NOK, as NOK frequently have many questions after receipt of the investigation, using any means available to obtain answers. Detailed and timely reporting, and close coordination between the reporting agent and the Family Liaison Coordinator will greatly assist in providing accurate information to the NOK and may preclude unnecessary conflicts between NCIS and the NOK.

30-22.8. The seizure and return of the victim's personal property is often a sensitive matter for the NOK. Coordination with the Family Liaison Coordinator, the CACO, and the victim's command can alleviate some of the NOK concerns and better assist the case agent concerning the disposition of the victim's property. The Family Liaison Coordinator retains the responsibility of informing the NOK concerning evidence custody procedures and expectations for final disposition of any personal property retained as evidence by NCIS. Providing the Family Liaison Coordinator with a list of all seized property has often proved beneficial.

30-22.9. Agents are reminded to coordinate all family liaison issues with the Family Liaison Coordinator, as this will greatly assist communication between NCIS and NOK and prove beneficial in alleviating misconception and misunderstanding. Close communication between NCIS and NOK has greatly reduced the number of congressional inquiries and misconception that the Navy/NCIS covers facts and circumstances surrounding the service member's death.

30-23. INTERVIEW OF VICTIM'S FAMILY MEMBERS. The impact of grief upon family members of a deceased victim can result in a highly charged emotional environment for an interview. Prior to the initial interview of the PNOK of the deceased victim (including an immediate family member), the case agent should apprise the NCISHQ 7H case reviewer of the preliminary details of the death investigation.

30-23.1. The interview of the PNOK should usually occur after the initial contact by the Family Liaison agent or the CACO. The Family Liaison agent or CACO can provide the case agent with the following information:

a. Address and telephone number of PNOK,

b. PNOK emotional and psychological well-being, and

c. Family concerns regarding the NCIS investigative process.

30-23.2. When family liaison is not conducted, the case agent shall contact the CACO prior to interviewing the PNOK. When the case agent desires family liaison advice, assistance may be requested from Code 23B. Documentation of specific statements made to the PNOK or family members is necessary to prevent misquotations and to preclude unwarranted conclusions. A request for investigative information by the PNOK shall be referred to the family liaison agent.

30-24. VIOLENT CRIMINAL APPREHENSION PROGRAM (VICAP)

30-24.1. Implemented by the FBI in concurrence with the National Center for Analysis of Violent Crime (NCAVC), VICAP is a nation-wide data information center designed to collect, collate, and analyze specific crimes of violence. Cases that meet the following criteria are accepted by VICAP:

a. Solved or unsolved homicides or attempts, especially those that involve an abduction; those which are apparently random, motiveless, or sexually oriented; or those which are known or suspected to be part of a series;

b. Missing persons, where the circumstances indicate a strong possibility of foul play and the victim is still missing; and

c. Unidentified dead bodies where the manner of death is known or suspected to be homicide.

30-24.2. Comparisons are made by analyzing modus operandi, physical evidence, suspect descriptions, etc. All NCIS homicide investigations or cases meeting the above criteria will be submitted to NCISHQ, Code 23B, using the VICAP Crime Analysis Report (FBI Form FD 676) to permit unsolved cases in the VICAP system to be evaluated for possible linkages to offenders. Forms are available from NCISHQ, Code 23B. The only exception to NCIS completing the form is in connection with reciprocal investigations; in those cases, a determination should be made regarding which agency (NCIS or the agency having primary investigative responsibility) will complete the form and the decision reported to NCISHQ. The form is normally submitted at the conclusion of the investigation; however, in some cases the form may be submitted earlier to allow for the determination by the VICAP staff of known information available to assist the early solving of the case.

30-25. MARINE SECURITY GUARD DEATHS. Investigations into the death of all Marine Security Guards (MSG) regardless of location will be conducted by NCISRA Quantico, VA. This is due to the necessity of conducting timely liaison with the command of the MSG at Marine Corps Base (MCB) Quantico, VA, and the ability of NCISRA Quantico agents to quickly obtain the necessary passport and visa for travel in completing in-country investigative steps. Any field office or resident agency that receives notification of the death of a MSG must immediately notify the SSA NCISRA Quantico by the most expeditious means. If that field office/resident agency is located in the country where the death occurred or in a nearby country that is easily accessed, NCIS special agents from that field office/resident agency should immediately respond to the scene. However, case control will remain with NCISRA Quantico. Additionally, the SSA NCISRA

Quantico will take immediate steps to augment the affected NCISRA by deploying an agent into the country where the death occurred. The SSA NCISRA Quantico will coordinate the request for additional assistance in those cases requiring additional skills (e.g., forensic consultant, MCRT). The SSA NCISRA Quantico will contact the NCISRA nearest the PNOK of the victim to arrange the initial interview within a reasonable amount of time after the death. This should be coordinated with the NCISHQ Family Liaison Coordinator. The above formal policy is specific to death investigations involving MSG, regardless of the cause and manner of death, and applies regardless, even if the MSG death occurs in a country where another NCIS field component is present.

30-26. COLD CASE MANAGEMENT

30-26.1. A cold case is defined as a death case wherein the manner of death has been ruled homicide or undetermined and all logical investigative leads have been exhausted without resolution. Consideration should be given to those death investigations which have not exhausted all investigative leads or identified a potential suspect to determine if the application of cold case methodology and protocol would increase the likelihood of resolution. Joint discussion between the field office management, NCISHQ Code 23B13 Cold Case Homicide Unit (CCHU), NCISHQ Code 23B SSA for Death Investigations, and the NCISHQ Code 23B Division Chief for Operations and Cold Case Investigations will determine if such a death investigation should be changed to a cold case investigation. Once identified as a cold case, a review will be conducted by NCISHQ Code 23B and the case agent to determine the proper tier level to be assigned to the case. This will determine the priority for the allocation of recourses and man-hours. An explanation of the Cold Case Tier System can be found in paragraph 30-26.7.

a. Cold cases are unique by the manner in which the investigations are conducted, managed, and maintained. Efforts are focused toward resolving the cases by utilizing established cold case methodology, protocol, and non-traditional methods.

30-26.2. For SSD entry, COLD CASE will be typed directly after the field in which the DEATH case category entry is typed at the top of the document, opposite the CCN entry. It will read as follows:

DEATH - COLD CASE

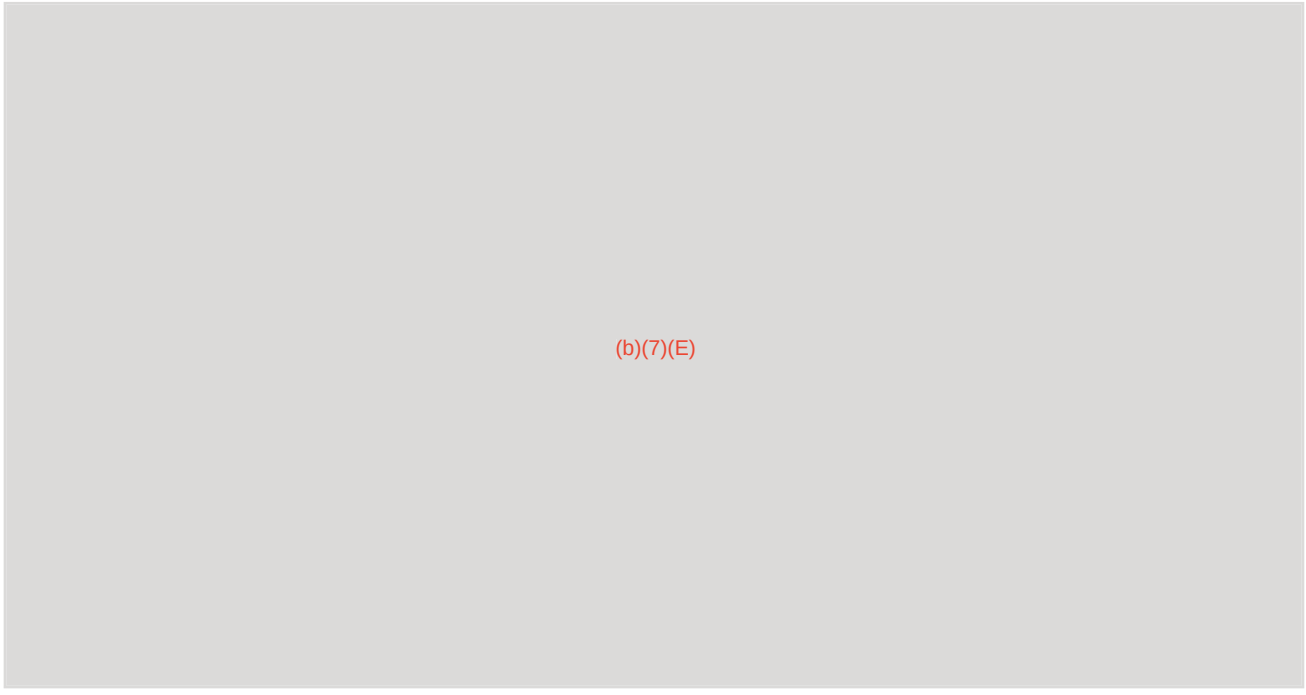
30-26.3. An unresolved homicide cannot be closed; however, if a cold case has been thoroughly investigated and all logical and non-traditional leads have been exhausted without establishing culpability, the case will be forwarded to NCISHQ Code 23B13 for review. The cold case agent will submit a ROI (INTERIM) documenting all leads conducted since the previous report. An ACTION to Code 23B13 will reflect that all logical investigative leads have been completed and request Code 23B13 conduct a review and authorize placing the case in an “inactive status” thereby exempting the Control Agent from all reporting requirements. NCISHQ CCHU will review the entire cold case investigation and respond to the field with a ROI (ACTION) indicating status of the review and final decision. If the NCISHQ CCHU agrees with placing the case in an “inactive” status, the original case file and evidence will be maintained by the control office unless otherwise directed by Code 23B13. Because unresolved homicide cases cannot be closed, evidence may not be destroyed. Periodic reviews must be conducted by the cold case

agent of all inactive cases in their AOR to determine if scientific or other advances would enhance resolvability of the investigation.

30-26.4. Due to the complexity of cold cases, two tier I and/or tier II cases will normally qualify as a full caseload for one cold case agent. If cases are simply awaiting prosecution or the majority of investigative activity has been completed, additional cold cases may be reactivated, opened or worked; however, discussion must take place between the field office and the NCISHQ CCHU prior to doing so. Cold case leads will routinely be conducted by cold case agents. Any selection of non-cold case agents for the conduct of the lead tasking must be coordinated with NCISHQ CCHU. All polygraph requests for cold cases must be coordinated with NCISHQ CCHU (the respective desk officer). A request will not be approved unless this coordination has taken place. Additionally, all psychological assessment requests must also be coordinated through NCISHQ CCHU. A ROI (ACTION) will task NCISHQ CCHU to coordinate the psychological assessment with Code 02D.

30-26.5. Sixty day ROI (INTERIM) reporting is required on all cold cases. Copies of all exhibits should be mailed to NCISHQ Code 23B13 (CCHU) to the attention of the respective Cold Case Desk Officer. As stated in 30-26.3, this reporting requirement does not apply to "inactive" cold cases or designated tier II or tier III cases. In addition, all cold case agents must submit a monthly update via email to their SSA and NCISHQ CCHU by the tenth of every month. These updates must be written in the Cold Case Monthly Update format provided by NCISHQ CCHU to all cold case agents and can also be found in the cold case section of the Code 23B website. These updates are vital to the Cold Case Program Manager's ability to provide weekly updates to the Executive Assistant Director (EAD) for Criminal Investigations on any cold case significant activity.

30-26.6. In order to maximize limited resources and to ensure optimum success in conducting cold case homicide investigations, the below tier system has been implemented. After an analytical review by NCISHQ Code 23B13 CCHU a case will be assigned to one of three tiers:



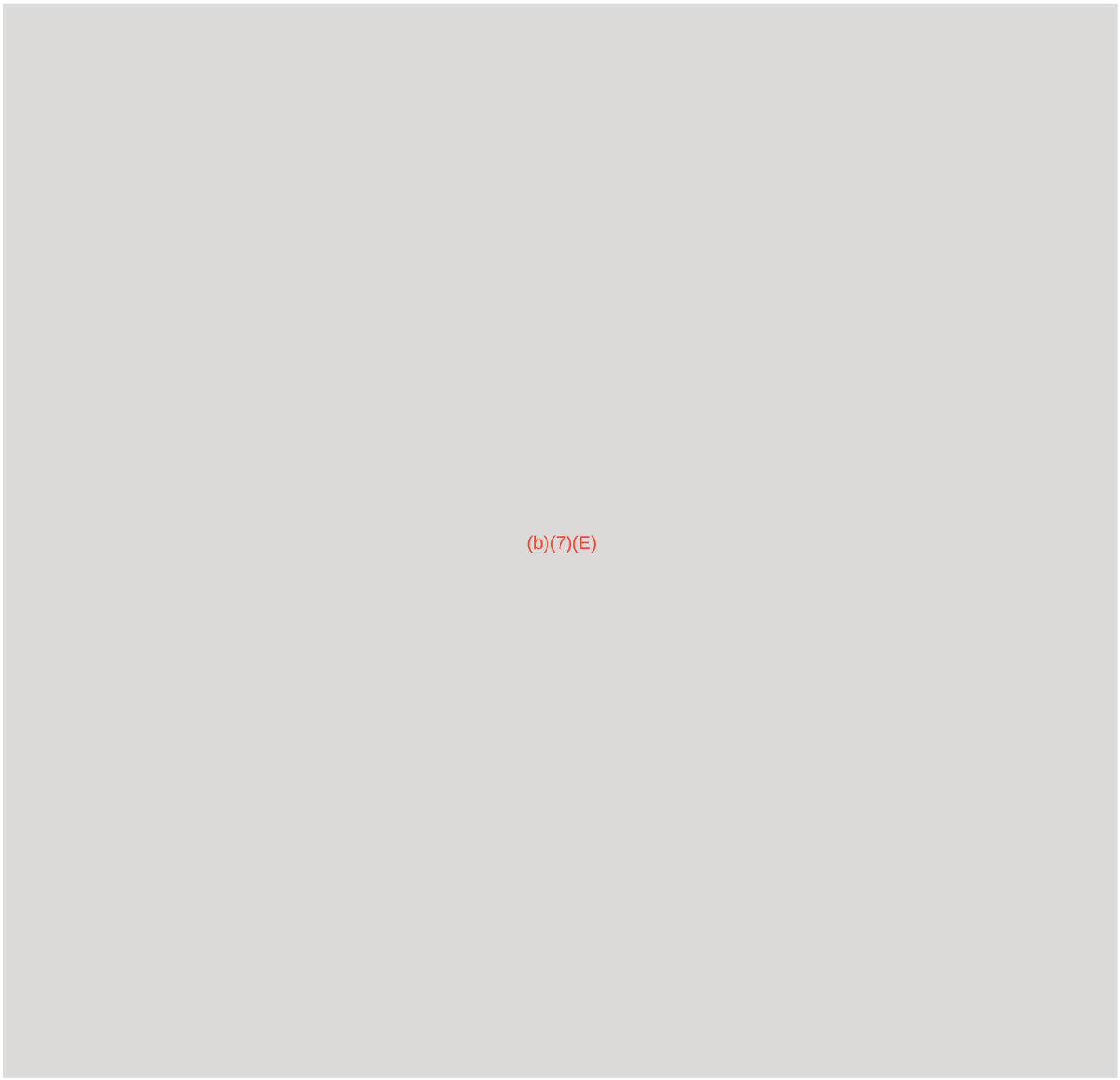
Pages 889 through 895 redacted for the following reasons:
- -
(b)(7)(E)

(b)(7)(E)

30-28. FATAL AIRCRAFT CRASHES AND OTHER SAFETY RELATED DEATHS. This section pertains to the division of labor when a death occurs impacting the DON by either mishaps or criminal activity. NCIS mission is to determine the facts of a death and pursue suspects when the death is ruled a homicide. The Commander, Navy Safety Center (COMNAVSAFECEN), headquartered in Norfolk, VA, has an equally time sensitive mission that requires investigation of mishaps, to include death cases, which have a serious impact on the DON. Safety investigations are time-proven methods to prevent further loss of life or equipment, as the COMNAVSAFECEN mission also impacts quality of life.

30-28.1. Personnel assigned to COMNAVSAFECEN possess technical expertise needed to investigate airplane crashes, death, and loss of property on board a ship or base and are obligated to initiate changes in the way the Navy does business when there is a concern for safety. Their operational demands are parallel to the mission of the Occupational Safety and Health Administration (OSHA) with the same lines of demarcation that exists between OSHA and federal, state, and local police existing between COMNAVSAFECEN and NCIS. In order that the quality of life in the Navy and Marine Corps be of the highest level possible, it is imperative that the two agencies coordinate efforts on matters when possible for the common good.

(b)(7)(E)



30-29. CONSPIRACY TO COMMIT MURDER

30-29.1. Elements of the Offense. According to the UCMJ, Article 81, the offense of conspiracy consists of:

a. That the accused entered into an agreement with one or more persons to commit an offense under the UCMJ; and,

b. That while the agreement continued to exist, and while the accused remained a party to the agreement, the accused or at least one of the co-conspirators performed an overt act for the purpose of bringing about the object of the conspiracy.

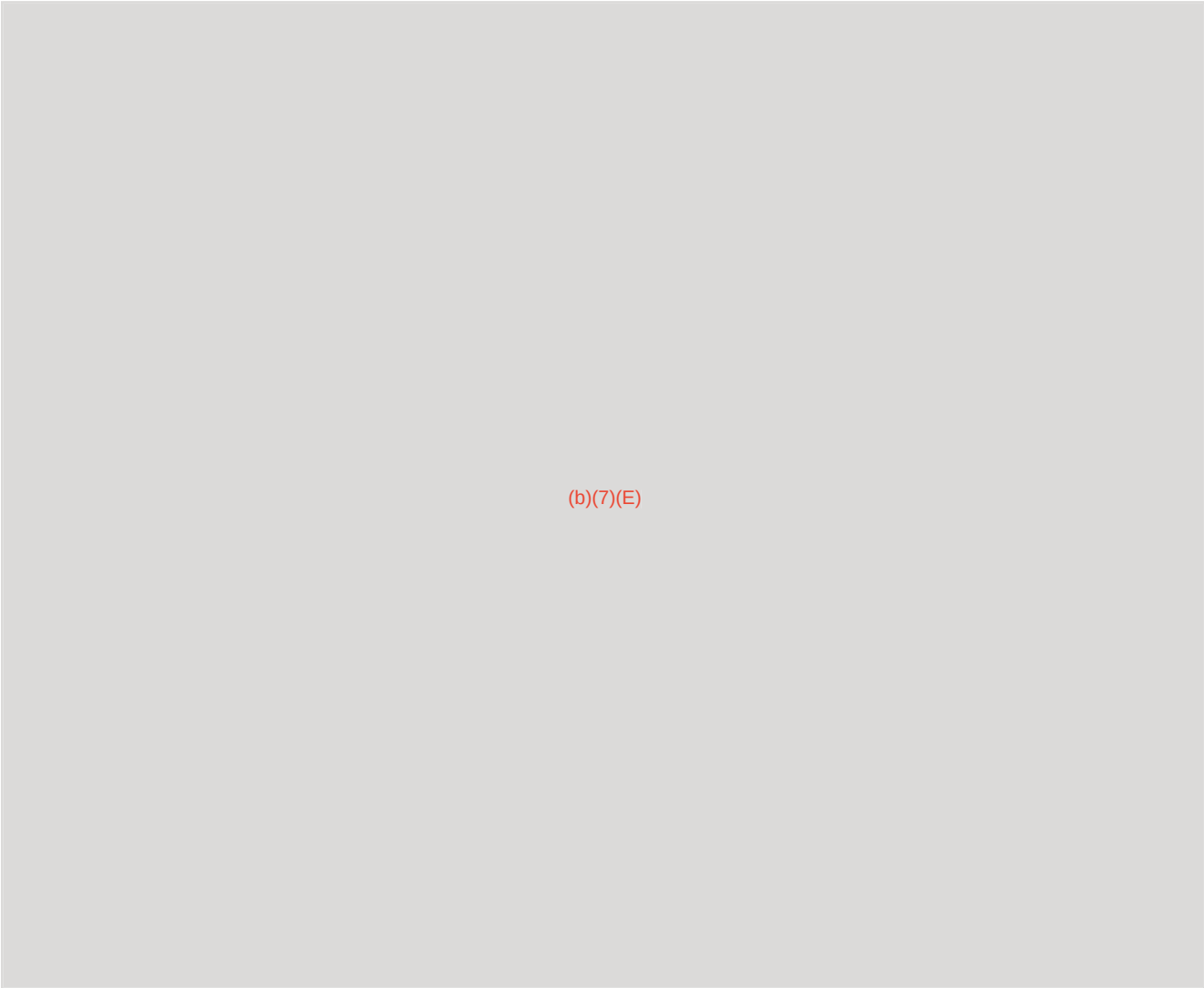
30-29.2. Conspiracy consists of two or more individuals who have agreed to accomplish an unlawful objective. Each conspirator is equally guilty of the execution of the conspiracy regardless of having knowledge of all the details of the crime or knowledge of the identity of co-conspirators.

a. Under the UCMJ, the accused must be subject to the code, but co-conspirators do not have to be subject to it. A person may be guilty of conspiracy although incapable of committing the intended offense. The joining of another conspirator after the conspiracy has been established does not create a new conspiracy or affect the status of the other conspirators. However, the joining conspirator must commit an overt act in furtherance of the agreement to be convicted of the offense.

b. Under the UCMJ, a member found guilty of conspiracy is subject to the maximum punishment authorized for the offense, and in no case shall the death penalty be imposed. The agreement in a conspiracy need not be manifested in formal words, but rather if the parties arrive at a common understanding to accomplish the object of the conspiracy, conduct of the parties will suffice. The object of the agreement must, at least in part, involve the commission of one or more offenses under the UCMJ. There cannot be conspiracy where the agreement exists only between the persons necessary to commit such an offense, e.g., dueling, bigamy, incest, adultery, or bribery. The overt act of a conspiracy must be independent of the agreement to commit the offense and must take place after agreement by one or more of the conspirators. If a party to a conspiracy abandons or withdraws from the agreement to commit the offense before the commission of an overt act by any conspirator then that party is not guilty of conspiracy.

30-29.3. Pursuant to SECNAVINST 5430.107, NCIS has jurisdiction in all major crimes (felonies) committed "against a person, the United States Government, or private property, including attempts or conspiracies to commit such offenses." This investigative jurisdiction includes major crimes on DON installations and ships involving military personnel, their dependents, and civilian employees.

(b)(7)(E)



30-30. SOLICITING ANOTHER TO COMMIT MURDER

30-30.1. Elements of the Offense. According to the UCMJ, Article 134, the offense of solicitation consists of:

a. That the accused wrongfully solicited or advised a certain person or persons to commit a certain offense under the code (other than those covered under Article 83, UCMJ);

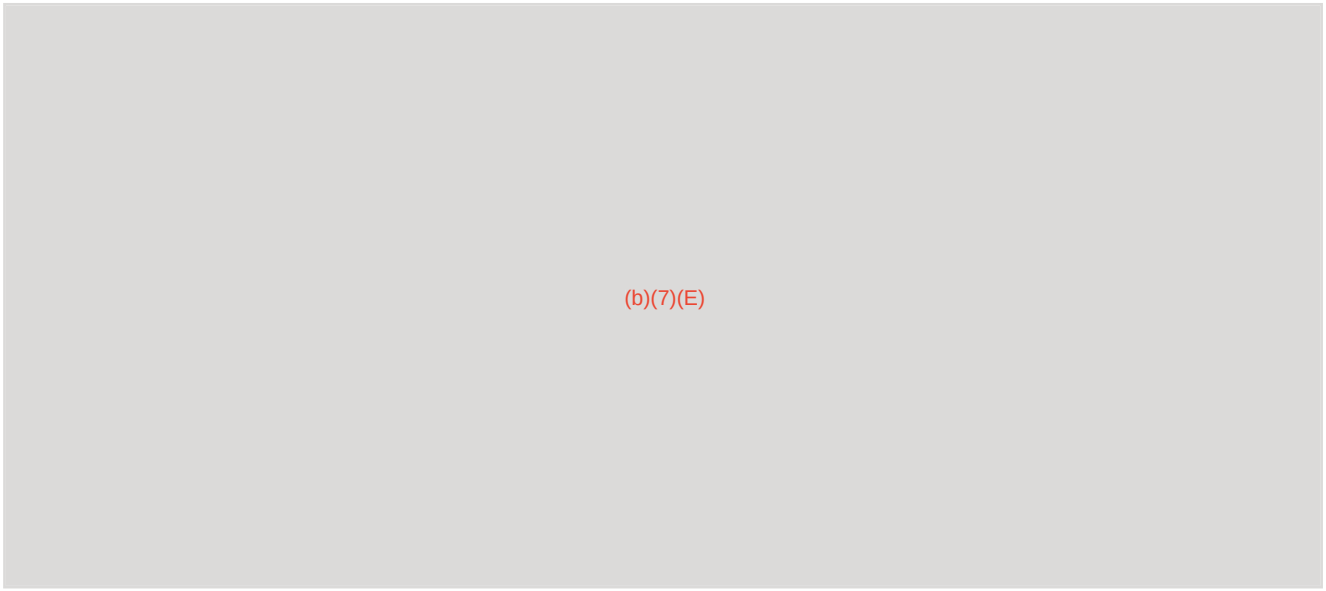
b. That the accused did so with the intent that the offense actually be committed; and

c. That under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the Armed Forces or was of a nature to bring discredit upon the Armed Forces.

30-30.2. Contemplating the commission of a crime is not an offense. Taking the first criminal step by soliciting one or more individuals to become involved in the crime is a punishable offense. The offense is complete when a solicitation is made or advice is given with the specific wrongful intent to influence another or others to commit an offense. The person solicited does

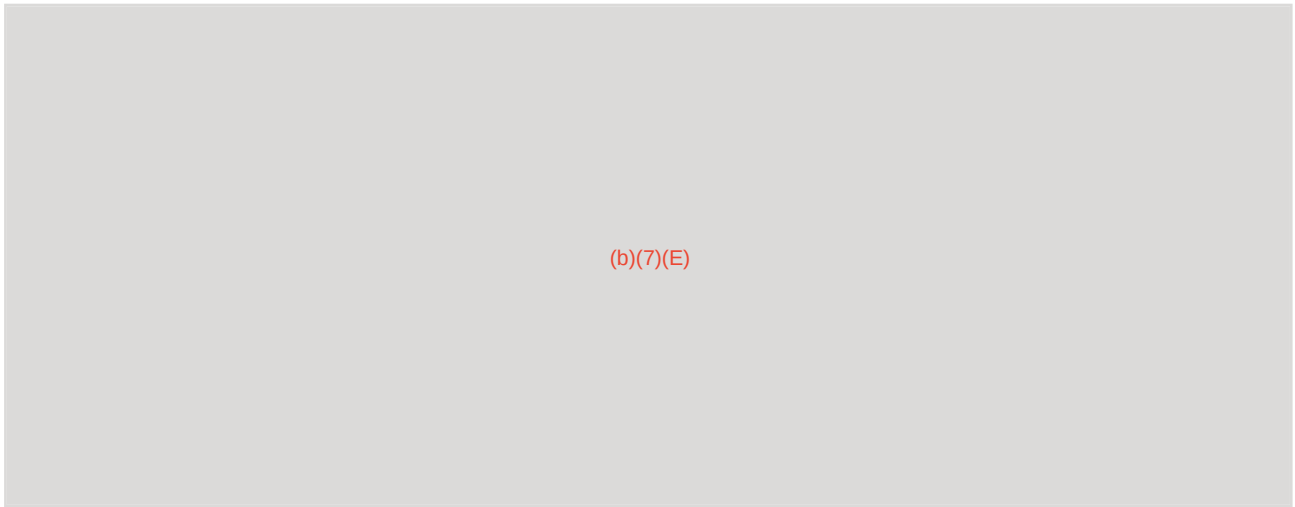
not have to agree to or act upon the solicitation. Solicitation may be by means other than word of mouth or writing and the accused may act through other persons in committing this offense. If found guilty, the accused shall be subject to the maximum punishment authorized for the offense solicited or advised, except in no case shall the death penalty be imposed nor shall the period of confinement exceed five years.

30-30.3. Pursuant to SECNAVINST 5430.107, NCIS has investigative jurisdiction in all major crimes (felonies), including solicitation, committed on DON installation and ships involving military personnel, their dependents, and civilian employees.



30-30.5. Title 18 USC Section 373, "Solicitation to commit a crime of violence," pertains to civilians suspected of solicitation to commit murder within NCIS jurisdiction.

30-31. DEATH INVESTIGATIONS IN HOSTILE ENVIRONMENTS AND FORWARD DEPLOYED SITUATIONS



Pages 901 through 904 redacted for the following reasons:
- -
(b)(6), (b)(7)(C)
(b)(7)(E)

APPENDIX (3): GLOSSARY OF MEDICO LEGAL TERMS

This is a list of key terms, words, and phrases commonly used in the field of forensic science. Knowing these terms will greatly enhance your effectiveness in investigations that involve death or injury. Also, this information will assist you to:

1. Understand terminology by medical personnel during examinations, autopsies, and case consultations.
2. Understand written medical reports pertaining to crimes of violence.
3. Question, if necessary, medico legal procedures that seem incorrect or incomplete, based upon the agent's unique knowledge of the specific case.
4. Communicate with medical and laboratory personnel in a professional manner.

The definition for each key term is necessarily brief. In many cases, where a single term has multiple meanings, only a shortened, medico legal definition is provided. These are basic, survival terms that every agent should know in order to contribute intelligently to the investigative process.

A

Abrasion: An injury caused by the scraping and removal of the superficial layer of the skin; also called scratches, grazed, or impact impressions.

Abrasion ring (Marginal abrasion): An injury to the skin that surrounds a projectile entry wound; the ring caused by the projectile entering the skin.

Adipocere: Soap-like or waxy substance formed during decomposition in moist environments.

Air embolism: An air bubble in a blood vessel.

Aneurysm: Degeneration with thinning and weakness of the wall of a blood vessel.

Antemortem: Before death.

Anterior: Located in front or nearer to the front of the body. Anterior, AKA Ventral.

Anoxia: Lack of oxygen.

Antecubital fossa: Forearm inside the elbow where blood is normally drawn.

Aorta: The largest and main artery of the body that originates at the heart and branches to distribute blood throughout the body.

Apex: The top of.

Arachnoid: The middle membrane that covers the brain between the "dura" membrane and "pia"

membrane.

Arterio-: Pertaining to the blood supply coming from the heart.

Artery: A thick-walled blood vessel that carries blood away from the heart.

Ascending: Going up.

Artifact (Artefact): An injury or object not related to the question at hand.

Asphyxia: Also called anoxia: A condition where airways or lungs have been mechanically blocked, or when air taken into the lungs lacks oxygen.

Aspiration: Breathing foreign material into the lungs.

Autopsy (Necropsy, Prosection): A detailed post-mortem medical examination.

Avulsion: The tearing away or pulling away of a structure or part.

B

Ballistics: The science dealing with the motion and impact of projectiles (bullets).

Beveling: A crater-like defect injury in the bone, usually the skull, that permits direction of force determinations in a gunshot wound; the crater appears on the side opposite of travel of the bullet.

Blanching: A light colored area that occurs in areas where the body comes in contact with a surface; blood vessel compression inhibits blood flow to those areas. Blanching can only occur before livor mortis (lividity) becomes fixed.

Blister: A collection of fluid separating the upper layers of the skin from the lower layers.

Buccal mucosa: The lining of the cheek wall.

C

Cardio-: Pertaining to the heart.

Cause of death: The disease, injury, or abnormality that alone or in combination is responsible for initiating the sequence of functional disturbances, whether brief or prolonged, that eventually ends in death. This is the underlying, proximate, or initiating cause of death. It may precede death immediately and thus be both the underlying and immediate cause of death, or it may produce other sequelae and complications that may be the immediate cause of death, the mechanism by which the underlying cause produces death.

Cervical: Pertaining to the upper vertebrae (neck).

Choking: A form of asphyxia, involving blocking the windpipe or squeezing the throat.

Clinical autopsy: A medical examination, usually only concerned with the cause of death.

Congestion: Excessive accumulation of blood in an area due to improper blood flow.

Conjunctiva: Pertaining to the delicate membrane that covers the exposed surface of the eyeball and the lines of the eyelid.

Constriction: Making smaller or narrower, especially at one place.

Contre-coup: A brain contusion located at the opposite side of the brain from the site of impact; a deceleration injury caused by the brain striking the interior of the skull common in falls.

Contusion: bruise; a blunt force injury caused by the crushing of soft tissues and the escape of blood to the surrounding tissues.

Coroner: A public official (not necessarily a physician) responsible in certain jurisdictions to determine the cause of death.

Coup: A brain contusion located directly under the site of impact; usually caused by a blow to the head.

Cranial suture: The fibrous joint between adjoining bones in the skull.

Cutaneous: Pertaining to the skin.

Cyanosis: A bluish discoloration of the skin, usually caused by a lack of oxygen in the blood.

D

Dermis: The live layer of skin, composed of connective tissue, located beneath the epidermis.

Diaphragm: The muscle that separates the thoracic cavity (containing the heart and lungs) from the abdominal cavity (containing the stomach and intestines): utilized in breathing.

Diaphysis: The shaft of a long bone.

Dilation: A widening or enlarging, usually to describe the pupils of the eyes.

Disarticulation: Amputation or separation of a limb at a joint.

Distal: Farther from the midline or point of attachment to the trunk; opposite proximal.

Distention: Expansion; swelling.

Dorsal: Pertaining to the back; posterior.

Dura mater: The tough, outermost membrane that covers the brain.

E

Ecchymosis: A hemorrhage, larger than a petechia, giving the appearance of a bruise.

Edema: An abnormal accumulation of fluid in the tissues; can cause swelling.

E.C.G. or E.K.G.: Electrocardiogram. A graphic recording of the electrical changes occurring during a cardiac cycle.

E.E.G.: Elecroencephalogram. A graphic recording of the electrical changes associated with the activity of the brain.

Embalming: The treatment of a dead body with disinfectants and preservatives to slow or prevent decomposition.

Embolism: A clot or foreign body that blocks a blood vessel.

En bloc: As a whole.

Epidermis: The outermost layer of the skin.

Epidural: On or outside the dura matter.

Epiphysis: The area of bone growth at the edge or end of a bone including the bulb-like structure at the end of a long bone.

Evisceration: Removing the internal organs; disemboweling.

Exhumation: The “digging up” and removal of a body from the burial site.

Exanguination: Extensive loss of blood due to a hemorrhage.

F

Foramen: A perforation or opening, especially through a bone.

Formalin: Substance used to preserve tissues or organs, and prepare them for microscopic or histologic study.

G

Gastric content: The matter (undigested food, etc.) found inside the stomach.

Gyrus: A convolution or elevation, usually referring to the structure of the brain.

H

Hematoma: A localized swelling created by blood.

Hemo-: Pertaining to blood.

Hemorrhage: The escape of blood from a blood vessel; bleeding.

Hemothorax: A condition where the chest cavity has filled with blood, usually as the result of trauma.

Hepato-: Pertaining to the liver.

Histology: The microscopic examination of tissue to detect normalcy, disease, trauma, or contamination, often conducted by a pathologist; also refers to the microscopic structure of tissue or other matter.

I

Incised wound: A cut; caused by drawing a sharp object across the skin; usually longer than it is deep; a sharp force injury.

Infarct: An area of dead tissue caused by the obstruction of normal blood flow to the part. A myocardial infarction is a heart attack.

Inferior: Beneath or under; ex: the chest is inferior to the head.

In situ: In the natural or normal place.

L

Laceration: A tearing or splitting of the skin or internal organ tissues due to blunt force trauma, not to be confused with an incised wound.

Lateral: Positional term designating a location away from the midline of the body or one of its organs or parts.

Lesion: An injury or change in an organ tissue that results in impairment or loss of function; a sore is a lesion of the skin.

Ligature: A constricting band (rope, wire, etc.) often used to cause asphyxia.

Ligature strangulation: Garroting; a form of asphyxia.

Livor mortis: Also post-mortem lividity; usually a purplish discoloration of the skin after death, caused by settling of the blood to parts of the body nearer to the ground.

M

Manner of death: A classification of the way in which the cause of death came about with special reference to social relationships and personal causation; the way in which the cause of death came about, whether by force of natural events, by accidental or suicidal self-infliction, or by other external forces. The usual classifications for manner of death certification are as follows: natural, homicide, suicide, accident, pending, and undetermined.

Manual strangulation: Throttling; a form of asphyxia caused by direct pressure of the trachea.

Marbling: The "marble-like" appearance of the skin due to the visibility of blood vessels under semitransparent decomposing skin.

Mastoid process: A bony prominence at the base of the skull, near the ear; sometimes used to determine sex from skeletal remains.

Maxilla: The upper jawbone.

Medial: At the midline, usually used to describe the location of the body.

Medical examiner: A public official, usually a physician, empowered by law to make cause and/or manner of death determinations.

Medicolegal autopsy: An autopsy that attempts to determine the cause of death, the manner of death, the time of death, and the identification of the deceased.

Mesentery: The tissue that attaches the intestines to the interior body wall.

Mummification: Decomposition of the body that results in tough leather-like tissues, caused by a dry environment (warm or cold).

N

Necrosis: Pathologic death of one or more cells.

Neural: Pertaining to the nerves.

Nuchal crest (External occipital protuberance): A bony prominence at the back of a skull; can be used in sex determinations from skeletal remains.

O

Odontology: A science dealing with the structure, growth, and diseases of the teeth; forensic odontology can be used for positive post-mortem identification.

Orbit-: The eye socket in the skull; interorbital distances and orbital shape can be used to help determine race.

Osteo-: Pertaining to bone.

P

Palpate: To massage or feel.

Pericardial sac: Sac around the heart.

Periorbital hematoma: Black eye.

Peritoneum: The membrane that lines the abdomen/pelvic walls.

Petechia: A pinpoint hemorrhage; sometimes seen in the eyes and organs in asphyxia-related deaths; can also be discovered in the face, the mucosa of the mouth and throat, the muscles of the temples, the pleural and epicardial surfaces, and the brain. Petechiae may also be found in non-asphyxial deaths.

Pia matter: The innermost of the three membranes that cover the brain, located under the arachnoid.

Pleura: The membrane enclosing the lungs.

Pneumo-: Pertaining to the lungs.

Pneumothorax: The presence of air in the pleural cavity, caused by injury to the lungs.

Posterior: Toward or at the back of the body.

Postmortem: Pertaining to occurring after death. Colloquialism for autopsy.

Prognathism: The degree to which teeth protrude from the jaws on profile; can be used to determine race.

Proximal: Nearer to the center of the body or to the point of attachment or origin.

Pulmonary: Pertaining to the lungs.

Putrefaction: Decomposition caused by bacterial action.

R

Renal: Pertaining to the kidneys.

Rigor mortis: The stiffening of the body after death due to chemical reactions in the muscle tissue.

S

Sclera: White of the eye.

Sloughing of the skin: The peeling away of skin, usually due to decomposition.

Stab wound: A sharp force injury, deeper than it is long.

Stellate: Star-shaped; stellate wounds can be created on the skin when a firearm is discharged while it is held in tight contact with the skull or sternum.

Subarachnoid: Located between the arachnoid membrane and the pia membrane in the brain.

Subarachnoid hemorrhage: Bleeding between the arachnoid membrane and the pia mater.

Subcutaneous: Under the skin.

Subdural: Under the dura membrane, between the dura membrane and the arachnoid.

Subdural hemorrhage: Bleeding between the dura and the arachnoid membrane.

Sulcus: A depression or trench; opposite the gyrus.

Superior: Above or on top of; ex: the head is superior to the chest.

T

Tardieu spots: Purplish spots caused by bleeding in the skin; observed in asphyxia victims; larger than petechiae.

Toxicology: The study of drugs and/or poisons and their effects on the body.

Trauma: An injury.

Tumor: An uncontrolled growth of tissue.

V

Vena cava: The major vein that returns blood to the heart.

Viscera: Internal organs.

Vital reactions: The migration of white blood cells into a traumatized area.

Vitreous humor: One of the fluids inside the eye; analysis of the vitreous often yields a reliable indication of blood chemistry at the time of death.

Pages 914 through 941 redacted for the following reasons:
- -
(b)(7)(E)

CHAPTER 31
TITLE: NARCOTICS AND DANGEROUS DRUGS (CATEGORY 7N)
POC: CODE 23A
DATE: MAY 08

31-1. DISCUSSION

31-1.1. General. This subcategory for narcotics and dangerous drugs is used to report investigative activity pertaining to violations of the Controlled Substances Act of 1970 and other anti-drug sections of Title 21 United States Code (USC), Chapter 13. Additionally, this subcategory is used for violations of Article 112a of the Uniform Code of Military Justice (UCMJ), to include unauthorized use, possession, and/or transfer of narcotics, controlled substances, and other dangerous drugs, as well as the unauthorized purchase, receipt, or introduction of the same into any Department of the Navy (DON) activity.

31-1.2. Definitions

a. Controlled Substance. Any substance that is included in Schedules I through V established by the Controlled Substances Act of 1970 (21 USC Section 812).

b. Schedule. Department of Justice (DOJ) and Federal Drug Administration (FDA) regulated classification levels (I through V) of drugs based on potential for abuse, accepted medical use, and potential for addiction.

c. Narcotic. Generic term referring to any illegal drug or unlawful possession of a drug. In legal context, refers to opium, opium derivatives, or synthetic substitutes, as well as cocaine or cocoa leaves as listed under the Controlled Substances Act (however, not technically a “narcotic” in medical sense).

d. Controlled Substance Analogue. A substance with a chemical structure substantially similar to the chemical structure and effect of a Schedule I or II controlled substance, but may or may not be a controlled substance. Also referred to as a “Designer Drug.”

31-1.3. Criminal Law/Jurisdiction

a. Uniform Code of Military Justice. Crimes of this category are potentially violations of the UCMJ:

Article 112a (Wrongful Use, Possession, Manufacture, Distribution, etc. of Controlled Substances)

Along with consideration for attempts and conspiracies.

b. Federal Laws/USC. Crimes of this category are potentially violations of Title 21 USC Chapter 13. Several sections within this USC Chapter deal with the various types of violations and circumstances. See the USC for specific and most current information. Violations within the USC should be considered for attempts and conspiracies. Crimes in this category that occur in federal jurisdiction, which are not directly covered under federal law but are violations under local or state law, may be potentially investigated though the Assimilative Crimes Act, Title 18 USC Section 13.

c. State Criminal Law. Depending on jurisdiction and/or victim/suspect of crimes of this category (i.e., non-military personnel or government property), appropriate state penal code may apply. Most of the individual states within the United States have adopted State Acts patterned after the Comprehensive Drug Abuse Prevention and Control Act of 1970. Therefore, under most jurisdictions, the control and enforcement of various narcotics offenses will be roughly parallel to this federal act.

31-2. POLICY AND GUIDANCE

31-2.1. Naval Criminal Investigative Service (NCIS) Authority. NCIS authority and jurisdiction to investigate this category of offenses are derived from SECNAVINST 5430.107. Department of Defense (DoD) Instruction 5525.07 implements the Memorandum of Understanding (MOU) between the DOJ and the DoD criminal investigative organizations. This MOU provides policy and guidance for criminal investigations when both departments have jurisdiction. See NCIS-3, Chapter 1 (Authority, Jurisdiction, Scope) for further explanation.

31-2.2. Overseas. There is no prohibition against NCIS investigating and arresting U.S. Navy/Marine Corps personnel serving abroad for violations of the UCMJ in drug-related offenses. Additionally, NCIS may participate in bilateral investigations in drug-related cases run in conjunction with local foreign police agencies, when directed at drug dealers or traffickers who are selling to U.S. Navy/Marine Corps personnel stationed abroad. Prior to initiating any operations, the Status of Forces Agreements (SOFA) and any other legal agreements between the host country and the U.S. should be reviewed. It may also be necessary to coordinate with the U.S. country team at the U.S. embassy of the host country, depending on the nature of the operation or investigation. However, NCIS must not take an active role in the actual arrest of any person not subject to U.S. law. In such bilateral operations, it is mandatory that NCIS personnel cooperating with local police do not deliberately involve themselves in the use of force, nor should they participate as members of an entry team or other active exercises of force in conjunction with the enforcement of foreign law.

31-2.3. DEA/NCIS Jurisdiction. Within the continental United States, the Drug Enforcement Administration (DEA), DOJ, has primary jurisdiction concerning all individuals involved in the trafficking of various types of drugs and narcotics. However, DEA normally does not concern itself with "routine" narcotics investigations of DON personnel. All NCIS components should be aware of the DEA primary jurisdiction, and must advise DEA representatives of any case

involving substantial trafficking of drugs or narcotics. In most locations outside the continental United States (OCONUS), the local (foreign) authorities have primary jurisdiction that they may or may not relinquish to DON authorities when U.S. personnel are involved. Usually, any narcotics investigations involving "on base" violations are investigated solely by NCIS components. In areas where the DON has primary jurisdiction, or in areas that do not have representatives of other organizations, NCIS components will investigate narcotic offenses, regardless of the complexity of the situations.

31-2.4. Under normal circumstances, any “on base” narcotics violation is investigated under the exclusive jurisdiction of the NCIS. However, this jurisdiction may be waived, in a case-by-case basis, in favor of a command-conducted investigation where the offense consists of simple possession of user amounts of marijuana, amphetamines, or barbiturates and/or the related presumptive use of these controlled substances where there is sufficient prima facie evidence present for the command to take appropriate action without NCIS investigative assistance, such as in the case of command urinalysis positive results. Additionally, as per SECNAVINST 5430.107 (Mission and Functions of the NCIS), NCIS may from time to time enter agreements into the use of Navy and Marine Corps command investigators (CID) in relation to initiating and conducting investigations, such as controlled substances investigations. These agreements, however, shall not prevent NCIS from assuming jurisdiction in the investigation of any offense.

31-2.5. NCIS Off Base Investigations. In concert with DoD Inspector General (DoD IG) policy document “Criminal Investigative Policy Memorandum Number 5 – Criminal Drug Investigative Activities” (OCT87), specifically involving “off installation” narcotics investigations, the NCIS will adhere to the following policy: The investigation of drug offenses outside the military installation normally is the responsibility of non-DoD law enforcement officials. That said, the following investigative actions outside military installations are authorized and may be conducted under regulations prescribed by the Secretary of the Military Department concerned, subject to the requirements set forth below:

a. NCIS investigative actions involving military members. Drug offenses by military members off installation, may be investigated to the extent authorized by the Manual for Courts-Martial (MCM), DoD Directive 5527.7 (reference C), rules issued by the Secretary of the Military Department concerned, and other applicable laws and regulations.

b. NCIS investigative actions involving persons “off installation” and not subject to the UCMJ. The Military criminal investigative organization may undertake investigative actions with respect to a person not subject to the UCMJ:

(1) If there are reasonable grounds to believe that a person has committed a felony drug offense in conjunction with a DON member.

(2) If there are reasonable grounds to believe that the person is the immediate source of the introduction of illegal drugs onto a military installation or facility.

c. All NCIS narcotics investigations conducted “off installation” will be coordinated with the appropriate prosecutorial authority and, wherever possible, run jointly with the cognizant law

enforcement authorities having primary jurisdiction in that area.

(b)(7)(E)

e. NCIS is authorized to purchase illegal drugs from persons not subject to the UCMJ and who are operating “off installation” when their transactions are believed to be targeting DON personnel.

f. NCIS may share information about illegal drug trafficking by non-DoD personnel to other civilian law enforcement officials and appropriate prosecutorial personnel.

31-2.6. Theft of Government Owned Narcotics/Controlled Substances. Thefts of government owned narcotics/controlled substances will be investigated under category 7N. Included are those thefts that have the elements of burglary/housebreaking, unless the circumstances clearly indicate that the narcotics theft was a secondary motive of the criminal act. The fraudulent procurement of government-owned narcotics/controlled substances, i.e., forgery of a prescription, fraudulent requisitions, will also be investigated under the 7N category. Warnings provided to subjects must encompass all suspected offenses.

31-2.7. NCIS will investigate allegations of pilfered or fraudulently procured government-owned narcotics/controlled substances regardless of value.

31-2.8. Investigations in General. If NCIS conducts an investigation involving narcotics or controlled substances, and it is a logical aspect of the investigation, a detailed crime scene examination should occur; to include photographs, diagrams/sketches, evidence collection, and taking statements. Attempts should be made to employ forensic techniques and/or technical support as appropriate.

31-2.9. The investigating agent should take written statements from suspects, witnesses, and when applicable, victims.

31-2.10. NCIS pro-active operations or initiative operations involving controlled substances are encouraged and are further discussed in NCIS-3, Chapter 9 (Criminal Operations).

31-2.11. If a NCIS investigation or operation is opened on controlled substances, liaison with the local security force and/or police departments of adjacent communities should occur, if it is a logical part of the investigation or operation. Any police reports or incident reports made by other law enforcement entities should be requested as part of the investigation.

31-2.12. Narcotics Awareness Briefings. All narcotics awareness briefings will be reported on the NCISnet, Web Applications Section, NCIS Brief Application, under case category 9Z. The NCIS Brief Application will provide a drop down menu to identify type of briefing, i.e., Narcotics. For additional information regarding the narcotics briefing program, please consult the following on NCISnet: http://infoweb.ncis.navy.mil/agency/briefings/Narcotics Brief.pdf.

31-3. ELEMENTS OF THE CRIME

31-3.1. Essential Elements. Any person subject to the UCMJ who wrongfully uses; possesses; manufactures; distributes; imports into the customs territory of the U.S.; exports from the U.S.; or introduces into an installation, vessel, vehicle, or aircraft used by or under the control of the armed forces a substance listed under the Controlled Substances Act (Title 21 USC Section 812) or listed on a schedule of controlled substances prescribed by the President of the United States has potentially violated Article 112a of the UCMJ.

31-3.2. Elements of Wrongful Possession, Use, Distribution, or Manufacture of Controlled Substances. The elements of Wrongful Possession, Use, Distribution, or Manufacture of a Controlled Substance under the UCMJ are as follows:

a. That the accused possessed, used, distributed, or manufactured a certain amount of a controlled substance; and

b. That the possession by the accused was wrongful.

31-3.3. Elements of Wrongful Introduction of a Controlled Substance. The elements of Wrongful Introduction of a Controlled Substance under the UCMJ are as follows:

a. That the accused introduced onto a vessel, aircraft, vehicle, or installation used by the armed forces or under the control of the armed forces a certain amount of a controlled substance; and

b. That the introduction was wrongful.

31-3.4. Elements of Wrongful Possession, Manufacture, or Introduction of a Controlled Substance with Intent to Distribute. The elements of Wrongful Possession, etc. with Intent to Distribute under the UCMJ are as follows:

a. That the accused possessed, manufactured, or introduced a certain amount of a controlled substance;

b. That the possession, manufacture, or introduction was wrongful; and

c. That the possession, manufacture, or introduction was with the intent to distribute.

31-3.5. Elements of Wrongful Importation or Exportation of a Controlled Substance. The elements of Wrongful Importation or Exportation of a Controlled Substance under the UCMJ are as follows:

a. That the accused imported into or exported from the customs territory of the U.S. a certain amount of a controlled substance; and

b. That the importation or exportation was wrongful.

31-3.6. Legal Discussion – Wrongful Use, Possession, Etc., of Controlled Substances. The investigating agent should consult the MCM and/or the UCMJ for the most current legal information regarding this violation.

a. Any of the above offenses potentially become aggravated (and possibly added as an extra element of the crime) if the accused was:

(1) On duty as a sentinel or lookout.

(2) On board a vessel or aircraft used by or under the control of the armed forces.

(3) At a missile launch facility used by or under the control of the armed forces.

(4) Receiving special pay (under Title 37 USC 310).

(5) At a time of war.

(6) In a confinement facility used by or under the control of the armed forces.

b. "Controlled Substance" means any substance which is included in Schedules I through V established by the Controlled Substances Act of 1970 (21 USC Section 812) and updated in the Code of Federal Regulations Part 1308. "Controlled Substance" includes amphetamine, cocaine, heroin, lysergic acid diethylamide, marijuana, methamphetamine, opium, phencyclidine, and barbituric acid, including phenobarbital and secobarbital.

c. "Possess" or "Possession" means to exercise control of something. Possession may be direct physical custody like holding an item in one's hand, or it may be constructive, as in the case of a person who hides an item in a locker or car to which that person may return to retrieve it. Possession must be knowing and conscious. Possession inherently includes the power or authority to preclude control by others. It is possible, however, for more than one person to possess an item simultaneously, as when several people share control of an item. An accused may not be convicted of possession of a controlled substance if the accused did not know that the substance was present under the accused's control. Awareness of the presence of a controlled substance may be inferred from circumstantial evidence.

d. "Distribute" or "Distribution" means to deliver to the possession of another. "Deliver" means the actual, constructive, or attempted transfer of an item, whether or not there exists an agency relationship.

e. "Manufacture" means the production, preparation, propagation, compounding, or processing of a drug or other substance, either directly or indirectly, or by extraction from substances of natural origin, or independently by means of chemical synthesis or by a combination of extraction and chemical synthesis; and includes any packaging or repackaging of such substance or labeling or re-labeling of its container. 'Production' includes the planting,

cultivating, growing, or harvesting of a drug or other substance.

f. "Wrongfulness" or "Wrongful." To be punishable under Article 112a, the possession, use, distribution, introduction, or manufacture of a controlled substance must be wrongful. Possession, use, distribution, introduction, or manufacture of a controlled substance is wrongful if it is without legal justification or authorization. Possession, use, distribution, introduction, or manufacture of a controlled substance is not wrongful if such act or acts are: (1) done pursuant to legitimate law enforcement activities (e.g., an informant who receives drugs as part of an undercover operation is not in wrongful possession); (2) done by authorized personnel in the performance of medical duties; or (3) without knowledge of the contraband nature of the substance (e.g., a person who possesses cocaine, but actually believes it to be sugar, not guilty of wrongful possession of cocaine). Possession, use, distribution, introduction, or manufacture of a controlled substance may be inferred to be wrongful in the absence of evidence to the contrary. The burden of proceeding with evidence with respect to any such exception in any court-martial or other proceeding under the code shall be upon the person claiming its benefit. If the evidence presented raises such an issue, then the burden of proof is upon the United States to establish that the use, possession, distribution, manufacture, or introduction was wrongful.

g. "Intent to Distribute" may be inferred from circumstantial evidence. Examples of evidence which may tend to support an inference of intent to distribute are: possession of a quantity of substance in excess of that which one would be likely to have for personal use; market value of the substance; the manner in which the substance is packaged; and that the accused is not a user of the substance. On the other hand, evidence that the accused is addicted to or is a heavy user of the substance may tend to negate an inference of intent to distribute.

h. "Certain Amount" refers to a specific amount of a controlled substance that is believed to be possessed, distributed, introduced, or manufactured by the accused. The specific amount should ordinarily be alleged in the specification. It is not necessary to allege a specific amount, however, and a specification is sufficient if it alleges that the accused possessed, distributed, introduced, or manufactured "some," "traces of," or "an unknown quantity of" a controlled substance.

i. "Use" means to inject, ingest, inhale, or otherwise introduce into the human body, any controlled substance. Knowledge that the substance is actually a controlled substance is a required component of use. Knowledge of the presence of the controlled substance may be inferred from the presence of the controlled substance in the accused's body or from other circumstantial evidence.

j. An accused who consciously avoids the knowledge of the presence of a controlled substance or the contraband nature of the substance is subject to the same criminal liability as one who has actual knowledge. This is also referred to as 'Deliberate Ignorance.'

(1) Example: A sailor is at a party where he is aware that other sailors are smoking marijuana in another room, but he purposefully does not go into the room and does not otherwise partake in the use of the controlled substance. This sailor, while not using controlled substances in that situation, went out of his way to avoid it but still has knowledge that other sailors were in

violation of Article 112a. If he does not report it, he risks being potentially accused of violating Article 112a if the other sailors who were using controlled substances were accused. The 'deliberately ignorant' sailor may also be potentially accused of violating Article 92 (Failure to Obey an Order or Regulation) of the UCMJ for not reporting the incident.

31-3.7. Legal Discussion – Other Military Offenses Related to Controlled Substances. As per SECNAVINST 5300.28D (05DEC05), the Secretary of the Navy instituted Military Substance Abuse Prevention and Control policy, which relates to, among other things, controlled substances and military personnel. Within this instruction there is a discussion of UCMJ Article 112a, as well as other related activities that may constitute a violation of UCMJ Article 92 (Failure to Obey an Order or Regulation). The following are potential violations of Article 92:

a. Drug Abuse Paraphernalia. Except for authorized purposes, the use, possession, or distribution of drug abuse paraphernalia by DON personnel is prohibited. Drug abuse paraphernalia under this instruction is similar to the Title 21 USC Section 863. See Drug Paraphernalia section below for further explanation.

b. Other Substance Abuse. The unlawful use by DON personnel of controlled substance analogues (designer drugs), natural substances (e.g., fungi, excretions), chemicals (e.g., chemicals wrongfully used as inhalants, aka "huffing"), propellants, and/or a prescribed over-the-counter drug or pharmaceutical compound, with the intent to induce intoxication, excitement, or stupefaction of the central nervous system is prohibited.

c. Deceptive Devices/Methods. The intentional acts to avoid providing a urine sample when lawfully directed; to dilute a urine sample to reduce the quantitative value of that sample when confirmed by mass spectroscopy and gas chromatography; to substitute any substance for one's own urine; or to chemically alter, adulterate, or modify one's own urine to avoid detection of any controlled substance; or to assist another in attempting to do the same is prohibited. See sections on Urinalysis and Fraudulent or Deceptive Urinalysis Screening below for further explanation.

31-3.8. Legal Discussion – Title 21 USC, Chapter 13. Title 21 of the USC deals with Food and Drugs, and Chapter 13 covers Drug Abuse Prevention and Control. This chapter is divided into two subchapters:

a. Control and Enforcement; and

b. Importation and Exportation.

31-3.9. The Control and Enforcement Subchapter is the principal portion of the chapter involving NCIS activity. This section defines various narcotics and dangerous drugs, and groups them into Schedules I through V, in descending order of potential danger as follows:

a. Schedule I: Those drugs with a high potential for abuse, which have no accepted medical uses in the United States. Examples include heroin, marijuana, and most hallucinogens.

b. Schedule II: Those drugs with legitimate medical uses, but which also have a high

potential for abuse. Examples include cocaine, selected barbiturates, some opiates, methamphetamine, amphetamine, and methaqualone.

c. Schedule III: Those drugs with lesser potential for abuse, and with legitimate medical uses. Examples include most stimulants (amphetamine-like) and the milder depressants (barbiturates).

d. Schedule IV: Those drugs such as the weaker barbiturates, sedatives, and tranquilizers which, although frequently prescribed, do have some abuse potential.

e. Schedule V: Those drugs with the lowest potential for abuse.

31-3.10. An important consideration for the NCIS agent regarding this federal statute is that an exchange of money is not required to constitute a trafficking offense. The penalties defined under this law are the same, regardless of whether there has been an exchange of money, since the law refers to the transfer of the substance rather than the sale.

31-3.11. Most of the individual states within the United States have adopted State Acts patterned after the Comprehensive Drug Abuse Prevention and Control Act of 1970. Therefore, under most jurisdictions, the control and enforcement of various narcotics offenses will be roughly parallel to this federal act. The federal law has the five (V) schedules; however, some states have added a "Schedule VI" to cover certain substances which are not "drugs" in the conventional sense, but that are nonetheless recreationally abused; these may include toluene (used in spray paints) and similar inhalants, such as amyl nitrate (aka 'poppers'), butyl nitrate, and nitrous oxide (found in aerosol cans).

31-3.12. Drug Paraphernalia. According to Title 21 USC Section 863, it is unlawful for any person to sell or offer for sale, or to use the mail (or similar service) to transport, or to import/export any kind of drug paraphernalia. Anyone convicted of this offense is subject to fines and imprisonment up to 3 years.

a. Drug Paraphernalia is defined as any equipment, product, or material of any kind which is primarily intended or designed for use in manufacturing, compounding, converting, concealing, producing, processing, preparing, injecting, ingesting, inhaling, or otherwise introducing into the human body a controlled substance. This includes items primarily intended or designed for use in ingesting, inhaling, or otherwise introducing marijuana, cocaine, hashish, PCP, methamphetamine, or amphetamines into the human body, such as (list not all inclusive):

(1) Metal, wooden, acrylic, glass, stone, plastic, or ceramic pipes with or without screens, permanent screens, hashish heads, or punctured metal bowls;

(2) Carburetion tubes, devices, pipes, and masks;

(3) Roach clips (objects used to hold small burning material, such as a marijuana cigarette);

(4) Miniature spoons with level capacities of one-tenth cubic centimeter or less;

(5) Pipes, such as water, chamber, electric, carburetion, air-driven, or ice;

(6) Bongs.

b. It should be noted that this does not apply to any person authorized by local, state or federal law to manufacture, possess, or distribute such items and any item that is traditionally used with tobacco products, including pipes, papers, and accessories are exempt.

31-3.13. Forfeiture. The use of forfeiture proceedings where warranted is encouraged. The forfeiture statutes are 18 USC Sections 1962 and 1963; 21 USC Section 848; and 21 USC Section 853. The following pertains to forfeitures in drug cases. NCIS-3, Chapter 40 (Forfeiture of Property), contains additional information.

31-3.14. Forfeiture is the taking, by the government, of illegally used or acquired property, without compensation to the owner. Under federal law, any money, conveyance (including cars, aircraft, or vessels), or equipment used with regard to the manufacture or transportation of a controlled substance is subject to forfeiture to the U. S. Government. This does not apply to property owned by a common carrier (e.g., a commercial airline) unaware of the presence of a controlled substance on or in its property. Forfeiture does not apply to property which has been stolen and then used for a criminal purpose. Under current law and practice, the agency that handles forfeitures for the U.S. Government in illegal drug cases is the DEA.

31-3.15. Generally, forfeiture proceedings in the United States are civil, not criminal proceedings. Once property is seized by a federal agent in an illegal controlled substance case, it must be appraised and placed in the custody of the DEA Regional Administrator. If the value of the property seized is $10,000 or less, it is subject to summary forfeiture, which requires that appropriate notice be given to the public in a local newspaper. If someone wishes to claim the property, they must: file a claim for the property, file a bond, petition for return of the property, and await the decision of the Chief Counsel of DEA. If no one responds to the notice, or if the petition fails, the property is disposed of per the DEA Regional Administrator's directions. If the property is of a value of more than $10,000, the notice must again be given and the case must be referred to a U.S. Attorney for review by the DOJ and possible judicial forfeiture action. Judicial forfeiture cases are usually titled as: The United States versus a piece of property; for example, "United States v. one 1982 Chevrolet Corvette." In judicial forfeiture cases, the government must merely show the court probable cause to believe that the property was used with regard to the manufacture or transportation of illegal drugs. Generally speaking, once probable cause is shown, the owner (property owners who are also criminal defendants do not appear in court to defend their property rights as a rule) of the property must appear in court and prove by a preponderance of the evidence that either:

a. The property was not in fact used in connection with illegal drugs; or

b. The property was used in connection with illegal drugs, but:

(1) The true owner is an unwitting common carrier;

(2) The property was stolen from the owner; or

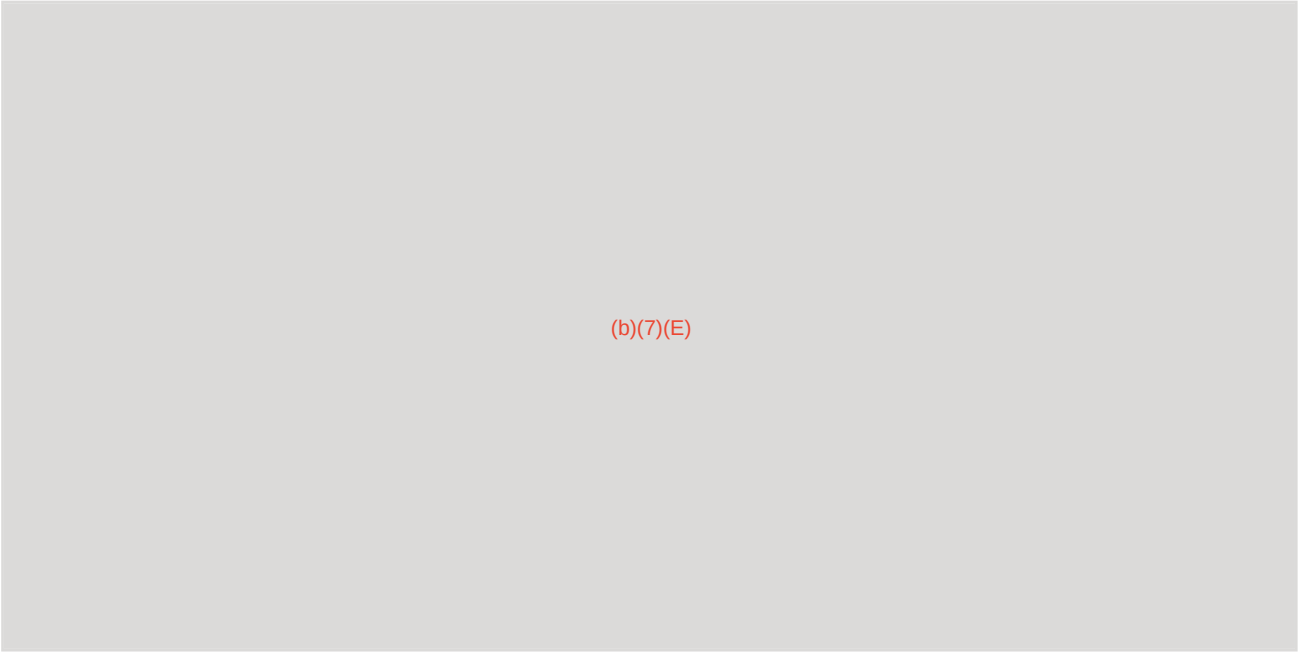
(3) The property fits into another statutory exemption.

31-3.16. Note that in judicial forfeitures the government has a very light burden of proof; the owner of the property has a heavier burden to show that the property in question was not used in a drug transaction (in the case of money) or that the property (car, glassware, equipment, etc.) was not used to transport or manufacture the illegal drugs.

31-3.17. From the foregoing, it can be seen that the potential number of seizures is enormous. Currency is involved in virtually every drug sale case. This currency is subject to forfeiture to the U.S. Government. A vehicle is involved in many transactions and simple possession cases. These vehicles may be the subject of forfeiture proceedings to the U.S. Government. The number of potential forfeiture cases actually presents a problem. DEA has developed guidelines that assist agents in deciding, on a case-by-case basis, whether forfeiture is appropriate.

31-3.18. NCIS special agents are encouraged, per local NCIS office guidance, to explore the possibility of using forfeiture procedures in appropriate cases. Because of DEA primacy in the drug forfeiture area, local liaison with DEA officials and U.S. Attorneys is mandatory. Not every case merits forfeiture of the personal property involved. However, the deterrent impact of a series of vehicle forfeitures, for example, in a particular area or on a particular installation, would be tremendous if given appropriate publicity. Negotiations with local counterparts will determine what can be accomplished. Use of this procedure has much promise as a tool in the Navy's war on drugs.

31-4. INVESTIGATIVE PROCEDURE



31-4.3. Limited Immunity. SECNAV Instruction 5300.28 (series) sets forth a program

encouraging any member of the DON with a drug abuse problem to obtain treatment or rehabilitation, as required, by means of self-referral. Military members who seek treatment or rehabilitation for drug abuse may initiate the evaluation and treatment process by voluntarily disclosing the nature and extent of their drug abuse to qualified drug screening personnel. Following disclosure, the screening activity will notify a member's commanding officer and recommend a course of treatment.

31-4.4. Disclosures made to appropriate drug screening personnel are privileged and may not be used against the member in any disciplinary action under the UCMJ. This limited privilege of disclosure also applies to the treatment process, as it involves both medical and non-medical drug treatment activities. Information disclosed by a member to persons other than drug screening, counseling, treatment, or rehabilitation personnel is not privileged. NCIS can initiate investigations regarding information developed through disclosure to non-drug screening personnel.

31-4.5. Urinalysis. Under current DoD regulations, urinalysis tests are conducted for two purposes: production of evidence for disciplinary purposes, and for the gathering of information to assist commands in combating drug and alcohol abuse. Urinalysis tests will be conducted expeditiously when commanders have probable cause to believe that a drug offense has been committed and there is probable cause to believe that evidence of the offense will be discovered by the testing. Military commanders may also consider urinalysis tests when a member is involved in events, incidents, or accidents that are out of the ordinary. Evidence of drug abuse discovered as a result of these urinalysis tests will not be usable for disciplinary purposes (unless probable cause also exists), but may constitute a basis for administrative separation. Finally, all urine samples tested positive by the portable urinalysis kits must be confirmed by a DoD Drug Screening Laboratory. When the results are intended for use as evidence in disciplinary proceedings, commands must maintain a chain of custody from the individual to the DoD laboratory. NCIS will normally not conduct an investigation based on urinalysis screenings unless the urine sample was obtained under conditions that will enable the results to be introduced as evidence in a court of law.

(b)(7)(E)

31-4.7. Should an individual request an exculpatory polygraph after one positive urinalysis test, the request will be honored, even if command contemplates administrative action only. Requests for such exculpatory examinations will be documented in a letter from an authorized requester to the servicing NCIS office. The letter will include the circumstances prompting the request, affirm the exculpatory nature of the request, and contain full identifying data of the subject.

31-4.8. An exculpatory polygraph request relating to a properly administered urinalysis test will not be approved if the subject admits to any in-service drug use, even though the transgression may have occurred many months prior to the pertinent urinalysis test. In this situation, the

subject would be eligible for command disciplinary action regardless of when the previously undisclosed in-service drug use occurred, precluding any need for a polygraph examination.

31-4.9. An exception to the above situation is when the subject admits in-service drug use for which he received disciplinary action, exemption, or treatment and denies use since that time. Therefore, if the subject was enrolled in a Navy drug exemption/rehabilitation program, then he can be polygraphed to cover the period following his entry into the program. If the subject has previously been exposed to military or civilian punishment for drug involvement while on active duty, then he may be polygraphed to cover the period following the adjudication date.

31-4.10. Fraudulent or Deceptive Urinalysis Screening. Civilian employers and military services have used urinalysis to detect the presence of illegal and abused prescription drugs in their applicants and/or employees for over a decade. With over 40 million Americans affected by drug screening, a thriving industry has developed which claims that their products will defeat urinalysis drug testing. The Internet provides a ready forum for these entrepreneurs to market their products. Recently, Navy and Marine Corps investigators have found, through sources and investigations, successful and unsuccessful attempts to mask and alter the results of drug screening. Several recent investigations involved urinalysis coordinators.

a. In light of the above, the following requirements for criminal investigations based on attempted or successful drug screening fraud now apply:

(1) For each ongoing and future investigation where fraud/deceptive practices were and/or are used to alter the results of any mandated DON urinalysis testing, provide an ROI (INFO) report to include:

(a) Reference the CCN of investigation

(b) Subject(s) age

(c) Subject(s) sex

(d) Subject(s) rank/rate

(e) Subject(s) duty assignment (what ship, shore installation, etc.)

(f) List products, chemicals and/or devices used

(g) Identify source of products, chemicals, and/or devices used

(h) Identify cases where subject(s) admit prior knowledge of unit sweeps and/or random testing or where known patterns of unit sweeps were common knowledge

(i) Identify cases where subject(s) used the Internet as source of information or to obtain products, chemicals and/or devices

(j) If the Internet is used, identify web sites subject used

(k) Violation(s) cited

(l) Unique circumstances/comments.

(2) Identify ongoing and potential future investigations where urinalysis coordinators were involved in requirement (1) above, and/or found to be taking bribes, providing information on unit sweep dates, or otherwise interfering with the urinalysis testing process. For each subject, provide the same information as noted in requirements (1) above and the violation(s) cited.

31-4.11. Military Working Dog (MWD) Program. The MWD Program is sponsored by the Chief of Naval Operations (N09N)/NCIS, but the operational control of individual MWD teams remains with the local commander. MWDs utilized by the Navy for physical security and law enforcement are usually of two types: patrol dogs and patrol detector dogs. The patrol detector dogs are further defined as patrol/drug and patrol/explosive. Like other highly specialized items of equipment, MWDs supplement and enhance the capabilities of security and law enforcement personnel.

31-4.12. Courts of law have ruled that MWDs provide probable cause for a search warrant when a positive finding is developed in the course of an MWD team search.

31-4.13. NCIS agents are not expected to accompany a MWD team during routine and random sweeps. In general, NCIS will assume investigative jurisdiction only if the quantities and types of drugs are within NCIS jurisdiction as defined in SECNAVINST 5430.107. A specific search may be completed by the MWD team, and any NCIS investigative effort might begin with receipt of the evidence from the MWD team.

31-4.14. For detailed policy and guidance on the MWD program, refer to OPNAVINST 5585.2 (series), Military Working Dog Manual.

31-4.15. Command Inspections and Inventories. In addition to narcotics investigations generated through the use of the MWD Program, NCIS is often requested to investigate individuals found to be in possession of illegal drugs during the course of command-initiated inspections and inventories. Military rules of evidence recognize command-conducted inspections that are reasonable in nature and deemed to be random. A regular schedule for these inspections need not be adhered to and frequency may vary. The inspections may cover all or part of a unit, but cannot focus on one individual or a limited group. These command inspections are conducted primarily to ensure the security, military fitness, or good order and discipline of the unit inspected. A unit commander may inspect specifically to locate and confiscate unlawful weapons or other contraband, to include controlled substances, if the commander can show reasonable suspicion that the property sought is present in the command or that the inspection was previously scheduled. An anonymous tip could be used to support reasonable suspicion if other circumstances support the information. Any evidence seized through such valid inspections is admissible at trial by court-martial.

31-4.16. Military rules of evidence have also determined that command-initiated inventories, if conducted to ensure safekeeping of the military member's personal effects in his absence, are valid, and contraband or illegal weapons thus found can be seized and used as evidence in legal proceedings. The inventory cannot be used as a subterfuge to cover an otherwise illegal search and NCIS cannot request an inventory of a subject's personal property for the purpose of determining that such evidence exists. In an inventory, only those items of obvious contraband may be seized. The observations of the person conducting the inventory may provide the probable cause necessary for the NCIS agent to obtain a search warrant or command authorization for search and seizure.

31-4.17. Suspected controlled substances discovered or recovered by command representatives can and should be forwarded by the command directly to the U.S. Army Criminal Investigations Laboratory (USACIL) in situations in which there are no substantive investigative leads requiring NCIS action. Coordination with the local NCIS office for other than intelligence purposes is not required.

31-4.18. Pharmaceutical Diversion. Diversion cases involve, but are not limited to, physicians who sell prescriptions to drug dealers or abusers; pharmacists who falsify records and subsequently sell the drugs; employees who steal from inventory, prescription forgers; and individuals who commit robberies, larcenies or break-ins at pharmacies, hospitals, medical clinics, and pharmaceutical distributors. The illicit diversion of pharmaceuticals from USN hospitals, clinics or pharmacies at USN/USMC facilities, or attached to expeditionary units is not uncommon. The diversion of pharmaceutical drugs often combines criminal activities commonly associated with fraud, larceny of government property and illicit drug trafficking. One possible indicator of pharmaceutical diversion may surface when a command inventory of narcotics reveals unexplained shortages of prescription drugs commonly associated with abuse or black-marketing. (b)(7)(E)

(b)(7)(E)

(b)(7)(E) When command reports to NCIS the loss of pharmaceutical inventories, consider advising the command to request a comprehensive audit by the Navy Audit Service (NAVAUDSERV), Washington, DC. The NAVAUDSERV can work collaboratively with command and NCIS to identify administrative irregularities that may isolate practices and personnel associated with past and on-going acts of diversion of pharmaceuticals.

a. Under federal law, all businesses that manufacture or distribute controlled drugs; all health care professionals entitled to dispense, administer, or prescribe them; and all pharmacies must register with the DEA. A registrant must maintain compliance with the regulations established by the DEA. Once the drugs are diverted, they can be sold on the street like any other drug; see section on Abused Prescription Drugs below for further explanation. Prescription drugs are commonly diverted to illegal use through:

(1) Fraudulent prescription by a legitimate provider or forged/altered by a patient;

(2) Over prescribing or indiscriminate prescribing by the provider;

(3) Illegal sale or distribution by health care workers;

(4) Robbery, larceny or break-in;

(5) “Doctor-shopping.” This term relates to a patient’s addiction or reliance on a certain prescription drug or treatment. Usually a patient will be treated by his/her normal physician and be prescribed a drug that is necessary for the legitimate treatment of his/her current medical condition. Once that condition has been successfully treated, however, most physicians will not continue to provide their patients with the medications they were taking. These patients will then actively seek out other physicians to obtain more of the same medication; often by faking or exaggerating the extent of their true condition in order to feed their addiction to that drug. In this context, the conditions mostly likely to be cited by patients are insomnia, anxiety, or pain.

31-4.19. Procedures. The following sections relate to procedures and guidance for case agents involved in narcotics and controlled substance investigations.

31-4.20. Article 31, UCMJ, Warning. Since the ultimate objective in any narcotics investigation is to identify and neutralize the source(s) of the drug/narcotics, the NCIS agent entering into a 7N-related interrogation must be prepared to cover all aspects of narcotic offenses (i.e., use, possession, and transfer or sale). Accordingly, the following violations will be identified to the subject at the onset of the interrogation, as offenses that he is suspected of:

"USE, POSSESSION, SALE, AND/OR TRANSFER OF MARIJUANA, NARCOTICS, AND DANGEROUS DRUGS."

In the event that the subject objects to any of these elements of the offense, the interviewing agent is free to explain that the fact that he is investigating all of these elements does not necessarily mean that the subject is guilty of all of the offenses.

31-4.21. Report of Investigation (ROI) Preparation. Only those aspects of ROI preparation which are peculiar to narcotics investigations will be addressed in this section.

a. Slang terms, such as "X," "rock," "hit," and "eight-ball," should be fully defined in all NCIS ROI narratives/statements. Probably all NCIS agents, and many of the people who are familiar with terminology involving narcotics offenses, are well aware of the meaning of these terms; however, many individuals who review NCIS reports may be unfamiliar with slang terminology. Additionally, the terminology fluctuates and could possibly have different meanings to different people, as well as having different meanings in different sections of the world.

b. Seizure Value. In order to fully explain the relative severity of the crime of possession of drugs/narcotics, it is important that the value of the seized drugs/narcotics be clearly set forth in the text of the ROI. It is not sufficient to set forth this figure in an exhibit only. Because of the tremendous fluctuation of "street value" of various drugs/narcotics from one area to another, the

responsibility of assigning the local seizure value rests with the reporting agent. In instances when the local "street value" differs considerably from the actual purchase price, both the purchase price and the "street value" will be reported (on a comparative basis). In all instances, the value should be calculated on the amount of narcotics actually involved and not the value of the amount further divided. Inflated recovery values detract from the professionalism and uniformity of reporting recoveries.

c. Frequently, a source of narcotics information will implicate numerous individuals in illegal narcotics activity. In these situations, a decision must be made whether to open a single case with multiple subjects or separate cases with single subjects. The following policy will apply:

(1) Persons committing, or conspiring to commit, narcotics violations together at the same time and place will be grouped into one case with one CCN. Persons not involved together in a single incident will be made the subjects of separate cases.

(2) An exception to this "one incident-one case" rule, is that a second case of the same category may not be opened on the same subject while the initial case is pending.

31-4.22. Narcotics Crime Scene Investigation. Crime scenes involving narcotics specifically or incidentally to another crime should be handled generally like all other crime scenes as outlined in NCIS-3 Chapter 6 (Investigative Theory and Procedure) and Chapter 12 (Physical Evidence and the Crime Scene). Along with photography, evidence collection, diagrams/sketches, interviews, etc., agents involved in a crime scene where narcotics are located should be cognizant of the following:

a. Officer/agent and crime scene safety, especially if at a narcotics lab/manufacturing site;

b. Precursor chemicals and/or equipment used in manufacturing or packing;

c. Drug paraphernalia and/or urinalysis masking agents or devices;

d. Documentation, such as ledgers, books, accounting, etc.;

e. Money or other potential profits of the crime (see section on Forfeiture above);

f. Cell phones, computers, pagers, etc.;

g. Weapons;

h. Literature on drug use, manufacturing, transporting, concealing, growing, etc.

i. Narcotics test kits (a.k.a. police field test kits) can be used on a scene to presumptively test for the presence of a controlled substance. Presumptive identification is generally legally recognized as a component for developing further probable cause. However, for evidentiary and possible prosecutorial purposes, the controlled substance must be seized in accordance with established evidence collection policy and tested at a certified forensic laboratory, such as the US

Army Criminal Investigation Laboratory (USACIL) or Armed Forces Institute of Pathology (AFIP).

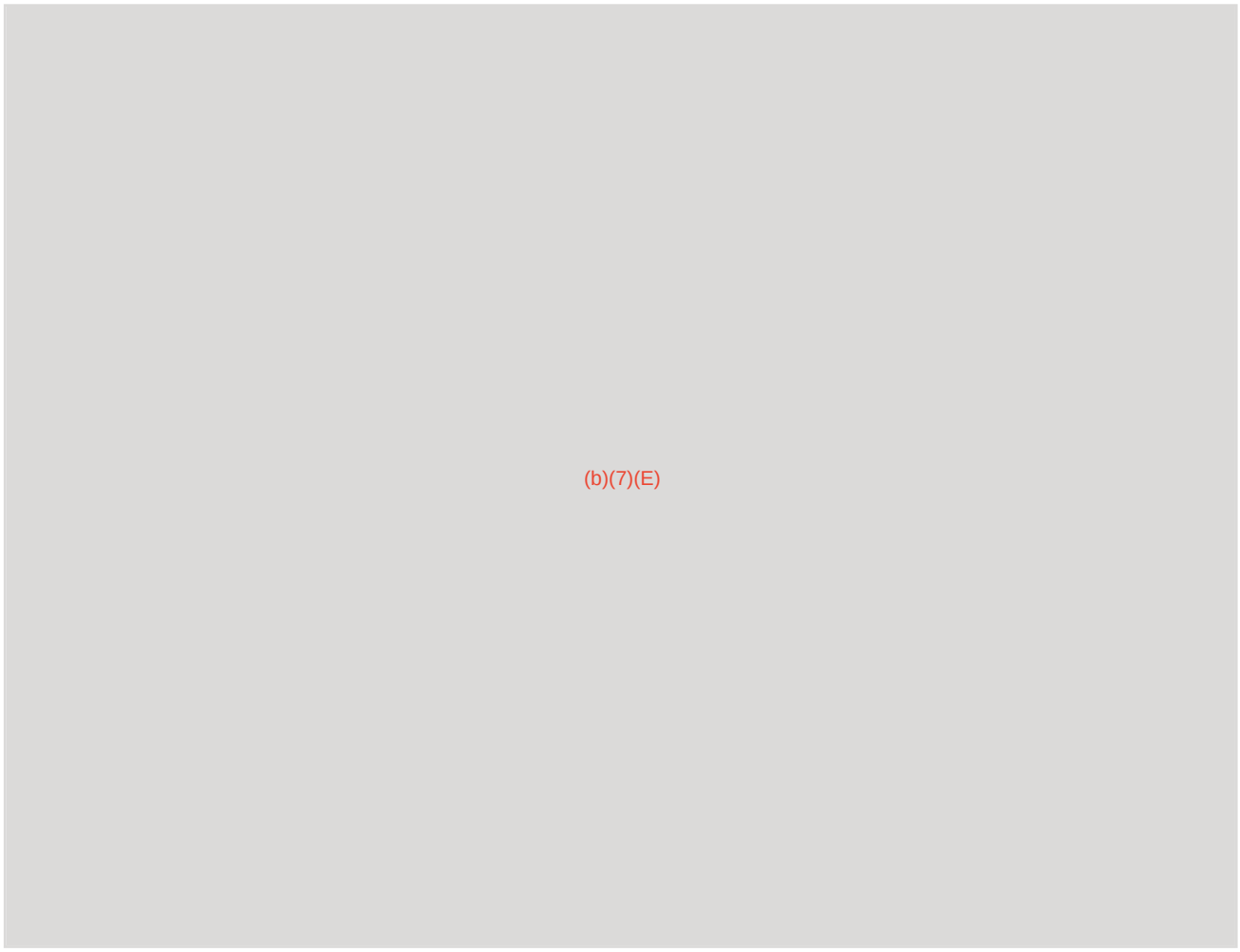
31-4.23. Investigation of Narcotics Offenses. There are four basic types of narcotics investigations that are conducted by NCIS: walk-in cases, allegation cases, possession cases, and narcotics purchases (uncontrolled, controlled, and NCIS agent purchases).

a. Walk-In Cases. An investigation wherein a service member makes unsolicited admissions of in-service involvement in narcotics. The investigative steps to be followed in this type of investigation are limited to an intensive, in-depth interrogation of the subject, and obtaining a permissive search waiver. The investigation will be terminated upon completion of the interrogation and attempted search. No attempts to exploit or corroborate admissions will be made, except in rare and extraordinary cases such as when the admission indicates an involvement so extensive as to preclude simple administrative processing by command or when serious security implications are presented. The investigator should be aware of the opportunity presented by the walk-in drug abuser in the area of narcotics intelligence. Attempts should be made to solicit as much criminal intelligence in these situations as possible.

b. Allegation Cases. An investigation wherein one individual accuses another of drug abuse. The investigative steps to be followed in this type of investigation include the execution of a sworn statement from the accuser and/or other witnesses, pursuit of all logical leads, followed by an interrogation of the subject of the investigation. During the course of this interrogation, an effort should be made to seek permission to conduct complete searches of the individual's residence/possessions. It is imperative that all NCIS components understand an effort toward obtaining a permissive search waiver is considered a logical lead in all 7N investigations. The only exception to this rule of seeking a permissive search waiver would be if the individual's belongings had been thoroughly searched by other authorities just prior to the interrogation. The fact that an individual may have been found in possession of a narcotic in another section of the ship or the base (e.g., during a vehicle search at the main gate), does not negate the necessity for seeking permission to search his person and belongings aboard the ship or station. One additional step to be considered in the allegation case is that of seeking authority to offer the subject a polygraph examination when appropriate.

c. Possession Cases. An investigation involving a subject who has been caught in possession of some suspected drug or narcotic. The steps to be followed in the possession case include obtaining the evidence under a proper evidence custody document, and obtaining a formal laboratory analysis of the substance. The next steps to be followed include the interview of all pertinent witnesses and, of course, the interrogation of the subject. Again, an effort to obtain a permissive search waiver must be effected. This also presents an excellent opportunity to collect current intelligence on area drug activity.

d. Narcotics Purchases. There are generally three types of purchase operations that can be utilized in narcotics investigations. See NCIS-3, Chapter 9 (Crime Reduction Operations) for more specific information on these types of operations. The following are summaries of the three types of narcotics operations:



31-4.24. Narcotics Evidence Destined for U.S. In order to satisfy requirements levied by the U.S. Customs Service, the following procedures are applicable when controlled narcotic substances are mailed to the U.S. from overseas for analysis or evidentiary purposes:

a. Narcotic substances must be sent by registered mail.

b. Packages will be double wrapped and clearly marked on both the inner and outer wrappers as containing evidence.

c. Packages will be mailed from one official address to another official address (never to an individual by name).

d. Packages will be mailed between NCIS components or will be addressed to a forensic laboratory, such as those of the USACIL, AFIP, DEA, or other federal laboratories.

e. NCIS components will immediately electronically transmit an ROI for NCISHQ Code 23, citing when the evidence/package was mailed, description of its contents, the address, and the registered mail number.

31-5. DRUG IDENTIFICATION

31-5.1. General. The Controlled Substances Act (CSA) regulates five classes of drugs; narcotics, depressants, stimulants, hallucinogens, and anabolic steroids. Each class has distinguishing properties, and drugs within each class often produce similar effects. The DEA website will provide the most current information on controlled substances and drug scheduling (see www.usdoj.gov/dea).

31-5.2. Narcotics (Opiates). Generally refers to drugs that produce morphine-like effects. These consist generally of opium, morphine, codeine, and thebaine, along with synthetic and semi-synthetic (e.g., heroin) narcotics.

a. The abuse of any opiate will usually be manifested by one or more significant side effects. The more frequent side effects of narcotics (opiates) are sleepiness, decrease in pain, decrease in cough effects, euphoria, confusion, depressed respiration, and constipation.

b. Narcotics (opiates) can cause a true addiction. In order to meet the criterion for addiction, the following four factors must exist:

(1) Tolerance - more and more of the drug must be taken to produce the same effect;

(2) Psychological dependence;

(3) Physiological dependence; and

(4) Withdrawal - usually occurs within six or eight hours after the last drug intake, and certain side effects are usually noted. The side effects most frequently observed include excessive sweating, nausea, a craving for sweets, a "goose pimple" condition of the flesh, tremors, and convulsions (possibly inducing death, especially in infants). Withdrawal is usually complete within 72 hours, and it is always concluded within a 10-day period. At the end of this 10 days, there will no longer be a physical dependence on the drug, but the psychological dependence may well remain, which tends to explain why so many individuals return to the drug.

31-5.3. Stimulants. The category of stimulants consists generally of amphetamine-type drugs (such as benzedrine, dexedrine, and methamphetamine), cocaine, methcathinone, anoretic drugs, and khat. Some of these drugs are illicitly referred to as "speed." Although they have legitimate uses, such as appetite suppressants, anti-depressants, etc., amphetamines are frequently abused by individuals who wish to remain awake or who are seeking a very excited "high." Amphetamines are not truly addictive because the abuser does not develop a physical dependence, but the potential for withdrawal syndrome is clinically recognized when drug use is stopped. However, a rapid tolerance is developed as well as a psychological dependence.

a. Agent Safety Note: Because of the combination of the violent attitude of the individual and his increased physical ability, the cocaine abuser is one of the most dangerous subjects for an agent to attempt to apprehend.

b. Cocaine, defined by law as a narcotic, is actually a powerful central nervous system stimulant. This substance is usually introduced into the system either by "snorting" (inhaling through the nasal passages), injection, or smoking.

c. Introduction of cocaine into the body system frequently produces one or more of the following results:

(1) Imagined increase in mental capability;

(2) Staves off fatigue, sleepiness;

(3) Decreased appetite;

(4) An excited feeling of euphoria;

(5) A dramatic increase in physical ability; and

(6) A tendency toward aggressive and violent behavior.

d. The introduction of cocaine by smoking or injection causes an almost immediate reaction; however, the "high" has only a short duration, and the individual who "crashes" from the "high" experiences a severe "come down." A strong psychological dependence develops for cocaine and the drug can produce a real psychosis, as well as a pseudopsychosis; this is especially true when a highly potent form of cocaine called "crack" is smoked.

e. An individual who has experienced an overdose of cocaine is likely to manifest one or more of the following symptoms:

(1) Severe headache;

(2) Stomach cramps;

(3) Hallucinations;

(4) Tremors and convulsions; and

(5) The "Cheyne-Stokes" syndrome, a condition wherein the individual appears to breathe very rapidly for a short period of time, followed by a long period of not breathing at all, followed by another short period of very rapid breathing.

31-5.4. Depressants. While alcohol is one of the oldest and most universal substances used as a depressant, many other substances have been developed that produce central nervous system depression. These drugs have been referred to as downers, sedatives, hypnotics, minor tranquilizers, anxiolytics, and anti-anxiety medications. Unlike most other classes of drugs of abuse, depressants are rarely produced in clandestine laboratories. Generally, legitimate pharmaceutical products are diverted to the illicit market. A notable exception to this is *gamma*

hydroxybutyric acid (GHB). Depressants consist generally of barbiturates, benzodiazepines, flunitrazepam, GHB, glutethemide, and methaqualone.

a. Barbiturates

(1) An individual who has abused barbiturates may exhibit one or more of the following symptoms; "drunken behavior," without the odor of alcohol, slurred speech, staggering gait, contracted/fixed pupils, impaired judgment, slowed reactions, and drowsiness.

(2) Continued abuse of barbiturates can result in true addiction on the part of the abuser, since all four factors of addiction are existent in the chronic abuser of barbiturates. These addiction factors include physical dependence, psychological dependence, development of tolerance, and the potential for withdrawal from barbiturates is more severe than from any other addictive drug known. This withdrawal usually begins within seven to ten days following termination of the introduction of the drug into the system. Convulsions, which are characteristic of this withdrawal, can and frequently do lead to death if the individual does not receive adequate medical attention. In addition, the classic withdrawal symptoms, listed under the section dealing with opiates, are also manifested.

(3) One additional problem with barbiturates is the situation referred to as "potentiation," wherein the combination of two or more depressant drugs produces a much more drastic effect than either of the drugs taken separately. For example, a combination of barbiturates with alcohol greatly intensifies the effect of both of the substances.

b. Methaqualone. Frequently referred to as "MX" or by the brand names Sopor and Quaalude. This drug is actually a hypnotic, which can cause true addiction, but its use produces depressant-like side effects. The abuse of this drug frequently results in irreparable damage to the kidneys and liver, and there are several documented cases of death from an overdose of Methaqualone.

c. Mood Altering Drugs. This category would normally be reserved for those drugs that would commonly be referred to as tranquilizers, such as Valium and Librium. Although there are no documented cases of an overdose death from these drugs, they are frequently abused and can result in very erratic behavior on the part of the abuser.

d. Other Substances of Abuse. The list of other substances of abuse is too long to address in this manual. However, the agent should be aware that such things as delirients, Darvon, and natural hallucinogens are existent, and do have potential for abuse.

31-5.5. Hallucinogens. Hallucinogens are some of the oldest group of drugs used for their ability to alter perception and mood. For centuries, many of the naturally occurring hallucinogens found in plants and fungi have been used to produce hallucinogenic affects. Synthetic hallucinogens that can be manufactured may be more common, some of which are much more potent than their naturally occurring counterparts. Drugs of this category are generally LSD, PCP, MDMA (Ecstacy), ketamine, psilocybin, peyote, and mescaline.

a. LSD

(1) LSD is technically known as d-lysergic acid diethylamide tartrate 25. Symptoms of abuse of LSD and other hallucinogens may include; unusual amount of uncooperativeness, mood alterations, irregular breathing, trembling, dilated pupils, chills, nausea, and hallucinations.

(2) The use of LSD and some other hallucinogens presents a unique danger of a flashback. Flashback from LSD has been documented as occurring more than twenty years after the introduction of the drug into the system. Utilization of LSD may also develop a tolerance to the drug and a cross-tolerance to other drugs. That is, it would take a proportionally higher amount of another drug similar to LSD, to produce the same results, because of having developed a tolerance to LSD. A distinct danger related to the use of LSD is birth defects, which have been medically documented, when one or both of the parents of the child utilized LSD prior to conception.

b. Phencyclidine (PCP)

(1) Agent Safety Note: Use extreme caution when handling suspected PCP or in dealing with subjects believed to be under the influence of PCP. Phencyclidine, commonly referred to as "Evil Weed" or “Angel Dust,” is legally manufactured as a veterinary anesthetic and illicitly produced in clandestine laboratories. PCP is commonly abused by oral ingestion of tablets, capsules, or powder form, alone and in combination with other drugs, and by smoking the drug after it has been sprinkled on parsley, marijuana, or some form of tobacco. Of particular note, PCP is often erroneously represented and sold as LSD, THC, or mescaline. Symptoms of abuse of PCP include, but are not limited to:

(a) Flushing,

(b) Profuse sweating,

(c) Analgesia,

(d) Involuntary eye movement,

(e) Lack of muscular coordination,

(f) Double vision, and

(g) Dizziness.

c. Natural Hallucinogens. There are several natural substances that can create hallucinations. These include:

(1) Psilocybin, commonly referred to as the sacred or magic mushroom.

(2) Peyote, which contains the substance mescaline, is derived from the blossom of a

particular type of cactus, native to the southwestern United States. Ingestion of mescaline causes hallucinations. It is legally ingested in the course of religious ceremonies by members of the Native American Church; however, only members of this religious organization are allowed to legally ingest mescaline, and they must do it only on religious grounds during religious services.

31-5.6. Cannabis (Marijuana)

a. Background. Technically referred to as Cannabis Sativa L, the marijuana plant has grown wild in most areas of the world since at least 3000 B.C. Cannabis is the plant from which hemp rope is produced throughout the world.

b. Cultivation and Identification. Certain regions of the world produce a plant with a higher concentration of tetrahydrocannabinol (THC), the psychoactive chemical contained within marijuana. The concentration of the THC in the plant is actually more dependent upon its growing environment than it is to genetic background. The plant itself reproduces annually and can be propagated by its own seeds. It may grow to a height of four to twenty feet, producing a squared stalk up to about two inches in diameter, and developing a leaf which is a palmate type containing an odd number of leaves having a serrated (saw toothed) edge.

c. The marijuana leaves contain cystolith fibers that resemble hair on one side of the leaf, and wart-like bumps on the other side. A forensic chemist who is familiar with the morphological characteristics of this plant can sometimes provide a presumptive identification by merely viewing a leaf under magnification.

d. Hashish is the resin of the marijuana plant, and although it ranges upwards of four times as expensive as plain marijuana, it is eight to ten times as strong (that is, it has eight to ten times the concentration of THC in an equivalent mass of substance). There are several methods of producing hashish from the marijuana plant, including soaking the entire plant in alcohol that extracts the resin, and then boiling away the alcohol, which leaves the residue (hashish). Another method is to dry and then press the entire plant under a great deal of pressure that exudes the resin which is then dried. "Hashish oil" is produced by a method similar to percolating coffee, wherein a quantity of marijuana is placed in a basket suspended above a liquid (usually alcohol), which is heated so it "percolates" the vegetable matter. Repeated replacement of the marijuana increases the concentration of the "hashish oil" which develops in the bottom of the pot. The most primitive method of producing hashish is simply to have a person walk through a marijuana field early in the morning when the dew is on the plant, and the resin which has oozed from the top of the plant simply collects on the body and is later scraped off and dried.

e. The use of either marijuana or hashish frequently produces two distinct stages of behavior in the abuser. The first stage is one of loud and boisterous behavior accompanied by a great deal of laughter and giggling. The abuser frequently then lapses into the second stage which may occur anywhere from 30 minutes to two hours later. This is a quieter and more meditative period. During this quiet period, the individual may become very melancholy, and there are documented cases of individuals developing suicidal tendencies during this meditative stage.

31-5.7. Anabolic Steroids

a. A general description for a family of over twenty compounds broadly defined as "any group of usually synthetic hormones that increase constructive metabolism, and are sometimes taken by athletes in training to increase temporarily the size of muscles and strength."

b. Anabolic steroids may be naturally occurring compounds such as testosterone, a male sex hormone, or they may be man-made compounds such as methandrostenolone. Steroids have legitimate uses other than to increase strength. The medical community uses steroids in replacement therapy for people who have had surgery and chemotherapy. They are also used to control bone and protein wasting diseases, and various forms of anemia.

c. There are problems associated with steroid use that range from the relatively mild to extremely serious. Reports from athletes utilizing steroids have shown complaints of dizziness, headache, faintness, anger, rage, and aggressive behavior. Steroid use has also been connected with an increase in retention of calcium, sodium, potassium, chloride, and phosphate, which in turn can lead to increases in skeletal weight, water retention, and bone growth. Serious side effects of steroid use can include:

(1) Jaundice,

(2) Kidney disorders,

(3) Increased cholesterol concentrations,

(4) Testicular atrophy and sterility,

(5) Iron deficiency anemia, and

(6) Edema.

d. The DON has traditionally prohibited the use of non-prescribed anabolic steroids by military personnel through regulatory general orders (OPNAVINST 5350.4 (series)). Violations of these regulations are punishable under UCMJ Article 92 (Failure to Obey an Order or Regulation). As of February 1994, a specific family of more than 20 "steroid" compounds was added to the Schedule III listing of the Controlled Substances Act.

31-5.8. Abused Prescription Medications. Certain legal medications or pharmaceuticals with legitimate uses are also placed under one of the Controlled Substances Act schedules. If these medications are wrongfully used, distributed, manufactured, possessed, etc. they can potentially constitute a violation of Title 18 USC Chapter 13 or the UCMJ. See section on Pharmaceutical Diversion above for more information. The following are examples of some of the more commonly abused prescription medications:

a. Schedule II narcotic substances and their common name (trade name) brand products include; hydromorphine (Palladone and Dilaudid), methadone (Dolophone), meperidine

(Demerol), oxycodone (OxyContin, Percocet and Percodan), fentanyl (Sublimaze and Duragesic), and morphine (MS Contin, Kadian and Avinza).

b. Schedule II stimulant substances and their common name (trade name) brand products include; amphetamine (Dexadrine and Adderall), methamphetamine (Desoxyn) and methylphenidate (Ritalin).

c. Schedule III narcotic include combination products containing less than 15 milligrams of hydrocodone per dosage unit (e.g., Vicodin) and products containing not more than 90 milligrams of codeine per dosage unit (e.g., Tylenol with codeine).

d. Schedule III non-narcotics include benzphetamine (Didrex), phendimetrazine, dronabinol (Marinol), ketamine, and anabolic steroids such as oxandrolone (Oxandrin).

e. Schedule IV narcotics include propoxyphene (Darvon and Darvocet-N 100).

f. Schedule IV substances also include alprazolam (Xanax), clonazepam (Klonopin), clorazepate (Tranxene), diazepam (Vallium), lorazepam (Ativan), midazolam (Versed), temazepam (Restoril), and triazolam (Halcion).

31-5.9. Laboratories. Clandestine laboratories are most commonly associated with hallucinogens, methamphetamine, and PCP. Any motivated person with some chemistry knowledge and access to the Internet is capable of researching and producing these substances. In addition, many of the businesses commonly referred to as "head shops" sell pamphlets and publications (e.g., Anarchist Cookbook) which contain the recipe for the production of various controlled substances. Safety is the most important point for the agent to remember in the investigation of a suspected clandestine laboratory.

a. Agent Safety Note: The agent should obtain assistance from a qualified forensic chemist and public health and safety officials prior to even entering a suspected laboratory. Avoid tampering in any way with the chemical workings inside the laboratory.

b. Illicit drugs often produced in clandestine laboratories include methamphetamine, amphetamines, MDMA (ecstasy), methcathinone, PCP, LSD, and fentanyl. There are generally two types of laboratories: the “super” laboratory and the “mom and pop” laboratory.

(1) Super laboratories are large, highly organized labs that account for 80% of all production of illegal drugs (e.g., methamphetamines, MDMA, etc.). For example, a methamphetamine “super” laboratory can produce 10 pounds or more of product per production cycle.

(2) Mom and pop laboratories generally manufacture 1 to 4 ounces per production cycle. Their operators generally produce enough for their own and close associates use and just enough extra to sell to others to finance the purchase of production chemicals.

c. When a clandestine drug lab is discovered, the investigating agent(s) should not conduct a

crime scene examination without first collaborating with fire officials, hazardous materials experts, public health officials, chemists, and environmental protection officials. The small labs ("mom and pop" type) are more associated with explosions, fires, uncontrolled hazardous waste dumping, and child endangerment situations.

(b)(7)(E)

CHAPTER 32
TITLE: ROBBERY (CATEGORY 7R)
POC: CODE 23A
DATE: SEP 07

32-1. DISCUSSION.

32-1.1. General. Robbery and its related offenses are property related crimes that also constitute a personal crime depending on circumstances, actions, and intent of the suspect.

32-1.2. Definitions.

a. Robbery. The taking of anything of value from a person against their will by means of force, violence, or the threat thereof.

b. Force or Violence. Actions taken, through intimidation or physical means, by which the accused deprives the victim of their property.

c. Fear. Reasonable perception of present or future injury.

d. Assault. Attempt or threat of bodily harm upon a person with unlawful force, regardless if the force or violence is consummated.

e. Battery. Injury or other contact upon a person in a manner likely to cause bodily harm.

32-1.3. Criminal Law/Jurisdiction.

a. Uniform Code of Military Justice. Crimes in this category are potentially violations of UCMJ:

Article 122 (Robbery)
Article 134 (General Article – Assault with Intent to Commit Robbery)

(1) Other potential violations, or lesser-included offenses, of the UCMJ related to the crime of Robbery are:

Article 121 (Larceny or Wrongful Appropriation)
Article 128 (Assault)

Along with consideration for attempts and conspiracies.

b. Federal Law/United States Code (USC). Crimes of this category are potentially violations of Title 18 USC Chapter 103 - Robbery and Burglary:

Section 2111 (Special Maritime and Territorial Jurisdiction)
Section 2113 (Bank Robbery and Incidental Crimes)
Section 2114 (Mail, Money or Other Property of the U.S.)
Section 2115 (Post Offices)
Section 2117 (Breaking or Entering Carrier Facilities)
Section 2118 (Robberies and Burglaries Involving Controlled Substances)
Section 2119 (Motor Vehicles)

(1) Along with consideration for attempts and conspiracies. Crimes in this category (on a larger scale) may also include violations of Title 18 USC Chapter 81, Sections 1651 through 1660 (Piracy and Privateering). Crimes in this category that occur in federal jurisdiction, which are not directly covered under federal law but are violations under local state law, may be potentially investigated through the Assimilative Crimes Act, Title 18 USC Section 13.

c. State Criminal Law. Depending on jurisdiction and/or victim of crimes of this category (i.e., government property), appropriate state penal code may apply. Examples of potential state penal code violations are Kidnapping, Armed Robbery (involves use of a weapon), Aggravated Robbery (involves use of a deadly weapon or appears to be deadly weapon), Highway Robbery or Mugging (crime takes place outside or in public place), and Carjacking (stealing a car from victim by force).

32-2. POLICY AND GUIDANCE.

32-2.1. NCIS Authority. NCIS authority and jurisdiction to investigate this category of offenses is derived from SECNAVINST 5430.107. The Department of Defense (DOD) Directive 5525.7 (Memorandum of Understanding between the Department of Justice and the DOD Criminal Investigative Organizations) provides policy and guidance for criminal investigations when both departments have jurisdiction. See NCIS-3, Chapter 1 (Authority, Jurisdiction, Scope) for further explanation.

32-2.2. NCIS Responsibility.

a. NCIS can investigate any suspected robbery to determine if it constitutes a robbery or other related crime, such as assault, burglary, larceny, etc.

b. The safety and well-being of the victim is paramount. The investigating agent(s) should ensure the needs of a victim are taken care of first before any significant interview or physical examination occurs.

c. If NCIS responds to a complaint of a robbery, a detailed crime scene examination should occur, to include photographs, diagrams/sketches, evidence collection and taking any

victim and/or witness statements. Attempts should be made to employ forensic techniques as appropriate.

d. Medical records (treatment, ambulance run sheet, mental health examination, etc.) will likely be important to the investigation. The investigating agent should make every effort to acquire all appropriate medical records. HIPAA (Health Insurance Portability and Accountability Act) prohibitions will likely apply and therefore written consent from the victim or other authorization will be necessary to get access to medical records. If necessary, consult with legal authority for information on acquiring medical records.

e. If an NCIS investigation is opened on a robbery, liaison with the local security force and/or police departments should occur. Any police reports or incident reports made by other law enforcement entities should be requested as part of the investigation.

f. The investigating agent should take written statements from the victim, pertinent witnesses, and from the interrogation of suspects.

32-3. ELEMENTS OF THE CRIME.

32-3.1. Essential Elements. With the offense of robbery under the UCMJ, the essential elements will involve force, violence, or threats and the deprivation of valued property from a person. Because of the nature of robbery, other potential offenses may be related such as kidnap, assault, or larceny. Under Federal and state laws, the definitions and elements of robbery may be different than in the UCMJ.

32-3.2. Elements of Robbery. The elements of robbery under the UCMJ are:

a. That the accused wrongfully took certain property from the person or from the possession and in the presence of a person named or described;

b. That the taking was against the will of that person;

c. That the taking was by means of force, violence, or force and violence, or putting the person in fear of immediate or future injury to that person's family, anyone accompanying the person at the time of the robbery, the person's property, or the property of a relative, family member, or anyone accompanying the person at the time of the robbery;

d. That the property belonged to a person named or described;

e. That the property was of a certain or of some value; and

f. That the taking of the property by the accused was with the intent permanently to deprive the person robbed of the use and benefit of the property.

If the robbery was committed with a firearm, the following element is added:

g. That the means of force or violence or of putting the person in fear was a firearm.

32-3.3. Legal Discussion – Robbery.

a. It is not necessary that the property taken be located within any certain distance of the victim. For example, if the suspect entered a house and, through threats of violence, forced the owner to disclose the location of valuables in an adjoining room and, leaving the owner tied up, went into the room to steal the valuables, the suspect has committed a robbery.

b. For a robbery to be committed by force or violence, there must be actual force or violence to the victim, preceding or accompanying the actual taking of the property against the victim's will. It is immaterial that there is no fear instilled into the victim. Any amount of force used which overcomes any actual resistance by the victim, or if the victim is put into a situation where no resistance is made, or the suspect overcomes resistance through immobilizing the victim, is enough to constitute a robbery.

c. It is not robbery if the article to be stolen is merely snatched from the hand of another or is taken through stealth and no other force is used and the victim is not in fear. However, if resistance is overcome through the act of the snatching, there is sufficient violence. For example; an earring torn out from a person's ear, or a victim is jostled by a confederate as a distraction so a pickpocket can take the victim's watch, or a person is knocked unconscious and their pockets are rifled through.

d. For a robbery to be committed by putting the victim in fear, there need be no actual force or violence, however there must be a demonstration of force or menace by which the victim is placed in fear and therefore warrants making no resistance. The fear must be a reasonable perception of present or future injury and the taking must occur while the victim is in this state. The perceived injury may be death; bodily harm; or destruction of property to the victim, or family member or relative of the victim, or to anyone in the victim's company at the time.

e. Robbery includes 'taking with the intent to steal'. Since larceny is an integral part of a robbery charge, there must be evidence in support of the larceny element. Stealing is the unlawful taking of another's property with the intent to permanently deprive the victim of that property. The specific value of the stolen property must be proved in a larceny; however, in a robbery the value of the property is not as important.

32-3.4. Elements of Assault With Intent To Commit Robbery. The elements of Assault with Intent to Commit Robbery under the UCMJ are:

a. That the accused assaulted a certain person;

b. That, at the time of the assault, the accused intended to commit robbery; and

c. That, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces or was of a nature to bring discredit to the armed forces.

32-3.5. Legal Discussion – Assault With Intent To Commit Robbery. An assault with intent to commit robbery is not necessarily the equivalent of an attempt to commit robbery. An assault can be committed with the intent to commit some offense without actually consummating the offense. For example, the fact that the accused intended to take money and that the victim had none is still an assault. See NCIS-3, Chapter 29 (Assault) for further details.

32-4. INVESTIGATIVE PROCEDURE.

32-4.1. General. The investigative procedures to be followed in robbery cases will be suggested by the circumstances of the particular case, and can be selected from those relating to other criminal offenses (e.g., Assaults) listed in this manual. The following additional suggestions are to assist an agent in the investigation of a robbery case; however, not all are applicable in all cases.

32-4.2. Crime Scene Search. Crime scenes of robberies may require additional technical examination. The following minimum requirements are essential in robbery investigations:

a. Identify the crime scene by exact location (barracks, ship, area, town, city, county, state, etc.).

b. Look for and collect physical evidence such as clothing, weapons, fingerprints, artifacts, foreign matter, blood, fibers, etc., left by the victim(s) and/or suspect(s).

c. Look for indications of violence (disturbed area, damaged furniture, broken glass, torn draperies, etc.).

d. Observe for any signs indicating forced entry (broken windows, cut screens, forced doors, locks, etc.).

e. Make a crime scene sketch noting location of victim/witnesses, suspects, and objects related to the crime in question.

f. Take appropriate photographs of evidence at the crime scene showing exact locations of each piece of evidence.

g. Re-enact the crime with use of witnesses/law enforcement officials.

h. Robbery attacks may involve cutting, stabbing, slashing, kicking, use of blunt force objects, or shooting. Investigate accordingly.

i. Determine if any security cameras in the area exist that may have captured the event.

j. Consider the use of advanced technical forensic methods, such as fingerprint examination, tool mark analysis, UV (black light) examination, psychological services, etc.

32-4.3. Interview of Victim. When interviewing the victim(s), the agent should remember the elements of the crime in framing their questions. At a minimum, the following information should be obtained during questioning of the victim(s) of a robbery:

a. What was the address or location, date, and time of the robbery?

b. What were the general circumstances of the robbery? What were the weather conditions?

c. What are the names and addresses of all witnesses? What were the victim(s) and persons with them doing at the time of the robbery?

d. How many robbers participated? What was the part played by each robber?

e. What were the complete physical characteristics and clothing apparel of each robber, including as many elements of description as the witnesses remember?

f. Did the robber(s) use force, violence, or intimidation? To what extent? Were they armed? With what type weapon(s)?

g. What were the movements and words of the robber(s) and their victim(s)? Has an attempt been made to reconstruct the crime?

h. What is the description of the property taken? Who were the owner and the custodian of the property? In whose possession was it at the time of the robbery?

i. Did the robber(s) take the property from the person or in the presence of the person robbed?

j. What route did each robber take upon leaving the scene of the crime?

k. What is the description of the car (if any) used by the robber(s)?

l. Were there any similar robberies in the vicinity?

m. Obtain a complete detailed statement of the incident from the victim(s).

32-4.4. Physical Examination. The following investigative procedures are to be pursued in robbery cases involving injury to victim(s) and suspect(s):

a. Obtain date, time, and place of victim's and/or suspect's treatment.

b. Note detailed description of all injuries (wounds).

c. List all treatment of suspect and victim, if any.

d. Obtain full identity of the examining medical officer, EMT professionals, first responders, etc.

e. Obtain estimate of recovery period of victim/suspect(s).

f. Take appropriate photographs (color/black and white), and construct body diagrams of all injuries.

g. Obtain a written medical report concerning the incident or doctor's statement if medical report(s) are not available (a hospital admission form is not sufficient). Keep in mind HIPAA prohibitions on release of medical reports.

32-4.5. Witnesses. Interviews and statements of witnesses will be similar to the interview of victim(s); however, the following leads should be covered during the robbery investigation. Conduct interviews of neighbors, associates, acquaintances, alibi witnesses, postmen, security guards, delivery drivers, and anyone else who is regularly in the crime scene area. Make sure victim's activities, suspect's activities (including aggressive activities), weapons, and sounds are covered during the above inquiries. Take detailed statements from witnesses to the robbery.

32-4.6. Identifying Data of Suspects. Obtain a detailed physical description of suspect(s) and their clothing, and distribute the identification to the base, station, and ship security. Make and distribute composite drawings and/or description of suspect(s) to appropriate commands and law enforcement agencies. The following items should be covered during identification data acquisition:

a. Physical description should include hair, eyes, ears, nose, age, race, weight, height, build, scars, tattoos, unique characteristics, etc.

b. Direction of escape, means, and weapon type(s) should be relayed to law enforcement agencies on and off base.

c. Description of items robbed (money, jewelry, valuables, etc.).

32-4.7. Evidence. When appropriate and logical, evidence should be obtained by NCIS agents during a robbery investigation. Instructions for handling of the evidence and its submission to the laboratory for examination are outlined in NCIS-3, Chapter 12 (Physical Evidence and the Crime Scene). It is important to advise the laboratory what kind of analysis is desired of the evidence being submitted along with a synopsis of the robbery investigation. The following are examples of physical and documentary evidence potentially useful in a Robbery investigation:

a. Physical Evidence:

(1) Photographs of victim's/suspect's wounds, scars, etc.

(2) Samples of blood, hair, etc., from victim(s)/suspect(s).

(3) Clothing of victim(s)/suspect(s).

(4) Weapons.

(5) Items with fingerprints, etc.

(6) Letters, notes, log books, motel registrations, etc.

b. Documentary Evidence:

(1) Laboratory reports.

(2) Crime scene report of facts.

(3) Crime scene sketch/map.

(4) Confessions.

(5) Witnesses' statements.

(6) Medical reports.

32-4.8. Searches. Following established criteria for the particular type of search is mandatory, such as consent, warrant, or command authorization. Prior to the search, the agent should consider what he is looking for in the particular search. Clothing, weapons, and fruits of the crime should be the primary considerations during a robbery search. See NCIS-3, Chapter 17 (Search and Seizure) for further explanation.

32-4.9. Witness Identification of Suspects. Line-ups, single suspect confrontations, and photographic identification (aka photo-lineups) are covered in the NCIS-3, Chapter 6 (Investigative Theory and Procedures); these identification methods are investigative tools available to help identify suspect(s) during a robbery investigation.

32-4.10. False Reports. The NCIS agent should be aware of false reports. There are numerous reasons for false reports: drunkenness, drug rip-off, custodian of missing funds, attention getting misconduct (self-inflicted injuries), sexual perversion, etc. If the evidence and statements of the victim do not fit the circumstances of the alleged crime, a false report may have been made. In the event of a false report the agent will warn the complainant for making a false official statement and/or false swearing; potential violations of UCMJ Articles 107 (False Official Statements) and/or 134 (General Article – False Swearing) and/or Title 18 USC Section 1001 (False Statements).

32-4.11. Modus Operandi. Some common robbery cases involve victims who drive taxi cabs, individuals who work at small stores or gasoline stations, individuals residing aboard the base in barracks, individuals hitch-hiking near or on the base, and individuals returning to their base residence from base activities. The method of robbery is usually by threat and assault to the

victim. The suspect(s) may be two or more individuals that flee the scene in different directions. Weapons employed are blackjacks, nun-chucks, knives, blunt objects (boards, pipes, etc.), razors, and hand-guns (often blank or starter pistols). The object of the robbery is money, jewelry, goods, or clothing. The assailant may strip the billfold of the victim's money, credit cards, and identification; discarding the billfold at or near the crime scene. Robberies commonly take place with one or two victims walking together in a secluded, dark area aboard the base or station. If the modus operandi is unusually characteristic, or if a series of similar robberies are encountered, consideration should be given to notify nearby law enforcement agencies of acquired criminal intelligence.

CHAPTER 33
TITLE: CRIMES AGAINST PERSONS – OTHER
POC: CODE 23A
DATE: APR 08

33-1. DISCUSSION

33-1.1. General. This chapter provides direction and discussion for the investigation of personal crimes not directly covered in other chapters of the NCIS-3 manual. Several different crimes are delineated in this chapter.

33-1.2. Definitions

a. Stalking. The intentional and repeated following or harassing of another person and who makes a credible threat, either expressed or implied, with the intent to place that person in reasonable fear of death or serious bodily harm.

b. Extortion. The obtaining of property from another induced by wrongful use of actual or threatened force, violence, or fear, or under color of official right.

c. Hate Crime. A crime motivated by racial, religious, gender, sexual orientation, or other prejudice, perceived or real, against the victim.

d. Perjury. The willful making of a false statement, while in a judicial proceeding, after swearing an oath to be truthful.

33-1.3. Criminal Law/Jurisdiction

a. Uniform Code of Military Justice (UCMJ). This chapter examines several crimes that are potentially violations of the UCMJ. See the section on Elements of the Crime (33-3.1) below for a list of the UCMJ Articles covered. All of the violations discussed in this chapter should be given consideration for attempts and conspiracies.

b. Federal Laws/United States Code (USC). Crimes of this category are potentially violations of Title 18 USC Chapters:

13: Civil Rights (in relation to Hate Crimes);

41: Extortion and Threats;
43: False Personation;
47: Fraud and False Statements;
55: Kidnapping;
73: Obstruction of Justice;
79: Perjury; and
110a: Domestic Violence and Stalking.

See the USC for specific and most current information. Violations within the USC should be considered for attempts and conspiracies. Crimes in this category that occur in federal jurisdiction, which are not directly covered under federal law but are violations under local or state law, may be potentially investigated through the Assimilative Crimes Act, Title 18 USC Section 13.

c. State Criminal Law. Depending on jurisdiction and/or victim/suspect of crimes of this category (i.e., non-military personnel or government property), appropriate state penal code may apply. Stalking and Hate Crime elements and definitions may vary greatly depending upon state penal code.

33-2. POLICY AND GUIDANCE

33-2.1. NCIS Authority. NCIS authority and jurisdiction to investigate these categories of offenses are derived from SECNAVINST 5430.107. DoD Instruction 5525.07 implements the Memorandum of Understanding (MOU) between the Department of Justice and the Department of Defense (DoD) criminal investigative organizations. This MOU provides policy and guidance for criminal investigations when both departments have jurisdiction. See NCIS-3, Chapter 1 (Authority, Jurisdiction, Scope) for further explanation.

33-2.2. Vehicular Accidents and Fatalities. A vehicular accident resulting in non life-threatening injury and in which the vehicle operator departed the scene without rendering assistance or making identity known , shall be investigated under Case Category 7T (Traffic Accidents). A vehicular accident that results in personal or government property damage wherein the vehicle operator flees the scene is also to be investigated under Case Category 7T. Vehicular deaths, whether the victim was the driver, passenger, pedestrian, or a combination thereof, will be investigated under the Case Category 7H (Death Investigations). NCIS-3, Chapter 30 (Death Investigations), section 30-15 (Vehicular Deaths) thoroughly discusses the investigative procedures for a 7H vehicular death.

33-2.3. Special Inquiry (7X). This subcategory is used for investigations within the basic category of “Crimes Against Persons” that pertain to matters of unique interest to the Department of the Navy (DON) and requiring the application of special investigative techniques or handling. This subcategory is also used for investigations, which, because of infrequent occurrence or for other reasons, are not specifically covered by any of the other crimes against persons (Category 7) subcategories. Investigative procedures will be dictated by the varying circumstances of the individual case. Special Inquiry (7X) type investigations include impersonation, attempted suicide, usury, obstruction of justice, stalking, and unlawful dissident activity.

33-2.4. Investigative Policy – Dissident and Protest Activities

(b)(7)(E)

33-2.5. Investigative Policy – Hate Crimes. NCIS does not normally investigative hate crimes as a separate, distinct offense under the UCMJ. Allegations of hate crimes should be investigated in accordance with recognized procedures for investigating the underlying or primary crime, for example, assault, rape, homicide, or housebreaking. However, an allegation of a hate crime may have an additional offense of Article 92 (Failure to Obey an Order or Regulation) added to the primary offense.

33-3. ELEMENTS OF THE CRIME

33-3.1. General. This section enumerates the elements and legal aspects of several different personal crimes not specifically covered in another chapter of the NCIS-3 manual. The following crimes under the UCMJ are discussed:

a. Article 127: Extortion (Category 7E);

b. Article 134: Communicating a Threat (Category 7E);

c. Article 134: Kidnapping (Category 7K);

d. Article 128: Child Abuse - Assault (Category 7L);

e. Article 131: Perjury (Category 7P);

f. Article 134: Subordination of Perjury (Category 7P);

g. Article 134: False Swearing (Category 7P);

h. Article 107: False Official Statement (Category 7P);

i. Article 134: Impersonating a Commissioned, Warrant, Noncommissioned, or Petty Officer, or an Agent or Official (Category 7X);

j. Article 92: Usury (Category 7X);

k. Article 134: Obstructing Justice (Category 7X);

l. Article 120a: Stalking (Category 7X); and

m. Article 92: Hate Crime (Category 7X or other appropriate personal crime subcategory).

NOTE: Article 92 (Failure to Obey an Order or Regulation) is in relation to violating Navy Regulations prohibiting such acts).

33-3.2. Elements of Extortion. The elements of extortion under the UCMJ (Article 127) are as follows:

a. The accused communicated a certain threat to another; and

b. The accused intended to unlawfully obtain something of value, or any acquittance, advantage, or immunity.

33-3.3. Legal Discussion – Extortion. The offense is complete upon communication of the threat with the requisite intent. Evidence of the actual or probable success or failure of the extortion need not be proved.

a. Threat. It may be communicated by any means but must be received by the intended victim.

b. Acquittance. Is the release or discharge from an obligation.

c. Advantage or Immunity. Unless it is clear from the circumstances, the advantage or immunity sought should be described in the specification. The intent to make a person do an act against their will is not, by itself, sufficient to constitute extortion.

d. A threat sufficient to constitute extortion includes a threat:

(1) To do any unlawful injury to the person (or property) of the individual threatened, or to any family member (or to any other person held dear);

(2) To accuse the individual threatened or to any family member (or to any other person held dear) of any crime; or

(3) A threat to expose or impute any deformity or disgrace, to expose a secret, or to do any other harm to the person, or family member or anyone held dear.

e. Communicating a Threat. The elements of communicating a threat under the UCMJ (Article 134) are as follows:

(1) The accused communicated certain language expressing a present determination or intent to wrongfully injure the person, property, or reputation of another person, presently or in the future;

(2) That the communication was made known to that person or to a third person;

(3) The communication was wrongful; and

(4) Under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces or was of a nature to bring discredit upon the armed forces.

f. Communicating a Threat – Legal discussion:

(1) To establish the threat it is not necessary that the accused actually intended to do the injury threatened. A declaration made under the circumstances which reveal it to be in jest, or for an innocent or legitimate purpose, or which contradict the expressed intent to commit the act, does not constitute the communication of a threat.

(2) This offense is not committed by the mere statement of intent to commit an unlawful act not involving injury of another.

33-3.4. Elements of Kidnapping. The elements of kidnapping under the UCMJ (Article 134) are as follows:

a. That the accused seized, confined, inveigled, decoyed, or carried away a certain person;

b. That the accused then held such person is against that person's will;

c. That the accused did so willfully and wrongfully; and

d. That, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces or was of a nature to bring discredit upon the armed forces.

33-3.5. Legal Discussion – Kidnapping

a. "Inveigle" means to lure, lead astray, or entice by false representations or other deceitful means. For example, a person who entices another to ride in a car with a false promise to take the person to a certain destination has inveigled the passenger into the car. "Decoy" means to entice or lure by means of some fraud, trick, or temptation. For example, one who lures a child into a trap with candy has decoyed the child.

b. "Held" means detained. The holding must be more than a momentary or incidental detainment. For example, a robber who holds the victim at gunpoint while the victim hands over a

wallet, or a rapist who throws his victim to the ground, does not, by such acts, commit kidnapping. However if, before or after such robbery or rape, the victim is involuntarily transported a substantial distance, as from a housing area to a remote area of the base or post, this may be considered kidnapping, in addition to robbery or rape.

c. “Against that person’s will” means that the victim was held involuntarily which may result from force, mental or physical coercion, or from other means, including false representations. If the victim is incapable of having a recognizable will, as in the case of a very young child or a mentally incompetent person, the holding must be against the will of the victim's parents or legal guardian. Evidence of the availability or non-availability to the victim of means of exit or escape is relevant to involuntary detainment, as is evidence of threats or force (or lack thereof) by the accused to detain the victim.

d. “Willfully” means the accused must have specifically intended to hold the victim against the victim's will to be guilty of kidnapping, rather than an accidental detention. The holding need not have been for financial or personal gain or for any other particular purpose. However, it may be an aggravating circumstance that the kidnapping was for ransom.

e. “Wrongfully” means without justification or excuse. For example, a law enforcement official may justifiably apprehend and detain, by force if necessary, a person reasonably believed to have committed an offense. An official who unlawfully uses that official's authority to apprehend someone is not guilty of kidnapping, but may be guilty of unlawful detainment. It is not wrongful under this paragraph and therefore not kidnapping for a parent or legal guardian to seize and hold that parent's or legal guardian's minor child. (See also section 33-3.6, Parental Kidnapping)

33-3.6. Parental Kidnapping

a. Both Article 134, UCMJ and 18 USC 1201 (Federal Kidnapping Act) explicitly exclude "parental kidnapping" and similar actions by a minor child's legal guardian.

b. Several states have statutes making parental kidnapping a criminal offense. A parent taking a child in violation of a custody decree may be punishable under Article 134, UCMJ. Also, a parent who takes a child in violation of a custody decree will frequently remove the child into another state in an attempt to avoid jurisdiction of the court originally granting the decree. In the Parental Kidnapping Prevention Act, Congress provided that parental kidnapping and interstate flight to avoid prosecution under applicable state felony statutes would be a violation of 18 USC 1073 (flight to avoid prosecution or giving testimony) and punishable by a fine of not more than $5,000 or imprisonment for not more than five years, or both.

c. NCIS special agents do not have the authority to take custody of minor children being held by a parent or legal guardian in violation of state law or court custody decree. Such instances fall within the jurisdiction of state agencies. (See also NCIS-3 Chapter 42, Missing Persons.)

33-3.7. Elements of Child Abuse (Assault). The elements of child abuse (assault) under the UCMJ (Article 128 - Assault Consummated by a Battery on a Child Under 16 Years) are as follows:

a. That the accused did bodily harm to a certain person;

b. That the bodily harm was done with unlawful force or violence; and

c. That the person was then a child under the age of 16 years.

33-3.8. Legal Discussion – Child Abuse (Assault)

a. Physical Abuse. Child physical abuse is any non-accidental injury to the child (e.g., striking, kicking, burning, biting the child), or any action that results in a physical impairment of the child. This may manifest as contusions, bleeding, fractures, subdural hematoma, and soft tissue injuries. Additional guidance in the detection/evaluation of physical injuries is provided later in this chapter. Abuse resulting in death is investigated under Category 7H (see NCIS-3 Chapter 30, Death Investigations). All sex related investigations and child pornography is investigated under Category 8B (see NCIS-3 Chapter 34, Sex Offenses).

b. Neglect. This is another form of child abuse, which is comprised of inadequate and/or improper care that resulted or could reasonable result in injury, trauma, or emotional harm. Neglect may include abandonment or failure to attend to the welfare of the child. A vital element in child neglect investigations is the degree of neglect amounting to the probable cause of the child's injury/bodily harm. Also included for consideration are the following circumstances of neglect:

(1) Failure to feed and clothe the child resulting in aggravated malnutrition (failure to thrive) or bodily damage through exposure to weather elements.

(2) Failure to secure available medical treatment for reasonably observable illness from which the child may be suffering, thereby producing complicated bodily disease or death.

(3) Failure to reasonably protect the child against a household nuisance (e.g., hot stove, poison, vicious animal, electric fan, etc.) resulting in injury to the child.

(4) Parental abandonment of the child in the home for periods of time and under circumstances that create a danger to the safety and well-being of the child.

33-3.9. Statute of Limitations for Child Abuse Offenses

a. Article 43, UCMJ, was amended to extend the statute of limitations for selected child abuse related offenses enumerated within the amendment to the time when the victim reaches the age of 25. The statute lists the following offenses as child abuse related offenses:

(1) Rape or carnal knowledge pursuant to Article 120;

(2) Maiming pursuant to Article 124;

(3) Aggravated assault or assault consummated by a battery pursuant to Article 128;

(4) Indecent assault, assault with intent to commit murder;

(5) Voluntary manslaughter, rape, or sodomy, or indecent acts or liberties with a child under Article 134.

b. Prosecutions for offenses covered by the amendment are barred if the statute of limitations period expired prior to 24NOV03, even if the victim has not attainted the age of 25. For all offenses that were not time-barred prior to the enactment of the amendment, the statute of limitation automatically becomes the date when the victim reaches the age of 25. As such, all evidence related to the above crimes must be maintained for a period of 25 years to ensure that these cases can be prosecuted until the statute of limitations has expired, unless the SJA or local prosecutor advises otherwise. The offense of rape enumerated in the amendment is not necessarily impacted by this amendment because Article 43, UCMJ, already provides that there is no statute of limitation period for offenses punishable by death. All sex-related offenses will be investigated under category 8B (See NCIS-3 Chapter 34, Sex Offenses for further information).

33-3.10. Elements of Perjury. The offense of perjury under the UCMJ (Article 131) has two subsections. Any person who in a judicial proceeding or in a course of justice willfully and corruptly;

a. Upon lawful oath or in any form allowed by law, gives any false testimony; or

b. In any declaration, certificate, verification, or statement under penalty of perjury (as permitted under Title 28 USC Section 1746) subscribes any false statement.

33-3.11. Elements of Giving False Testimony. The elements of giving false testimony (perjury) under the UCMJ (Article 131) are as follows:

a. That the accused took an oath or affirmation in a certain judicial proceeding or course of justice;

b. That the oath or affirmation was administered to the accused in a matter in which an oath or affirmation was required or authorized by law;

c. That the oath or affirmation was administered by a person having authority to do so;

d. That upon the oath or affirmation that the accused willfully gave certain testimony;

e. That the testimony was material;

f. That the testimony was false; and

g. That the accused did not then believe the testimony to be true.

33-3.12. Elements of Subscribing a False Statement. The elements of subscribing a false statement (perjury) under the UCMJ (Article 131) are as follows:

a. That the accused subscribed a certain statement in a judicial proceeding, or course of justice;

b. That in the declaration, certification, verification, or statement under penalty of perjury, the accused declared, certified, verified, or stated the truth of that certain statement;

c. That the accused willfully subscribed the statement;

d. That the statement was material;

e. That the statement was false; and

f. That the accused did not then believe the statement to be true.

33-3.13. Legal Discussion – Perjury. For this article to apply, the accused must have committed this offense during or relating to a judicial proceeding or in the course of justice. In general, "judicial proceeding" includes a trial by court-martial and "course of justice" includes an investigation conducted under Article 32.

a. Giving False Testimony. The testimony must be false and must be willfully and corruptly given; it must be proved that that accused gave the false testimony willfully and did not believe it to be true. The false testimony must be with respect to a material matter, but not necessarily the main issue in the case. The falsity of the allegedly perjured statement cannot be proved by circumstantial evidence alone, except with respect to matters, which by their nature are not susceptible of direct proof. The falsity of the statement cannot be proved by the testimony of a single witness unless that testimony directly contradicts the statements and is corroborated by other evidence, direct or circumstantial, tending to prove the falsity of the statement. However, documentary evidence directly disproving the truth of the statement charged to have been perjured does not require corroboration if:

(1) The document is an official record shown to have been well known to the accused at the time the oath was taken, or

(2) The documentary evidence originated from the accused or had in any manner been recognized by the accused as containing the truth, before the alleged perjured statement.

b. Subscribing a False Statement. Title 18 USC Section 1746 provides for subscribing to the truth of a document by signing it expressly subject to the penalty of perjury. The signing must take place in a judicial proceeding or course of justice. It is not required that the document be sworn before a third party.

33-3.14. Subornation of Perjury. Allied to perjury, and punishable under Article 134 of the UCMJ, is Subornation of Perjury, which consists of influencing, persuading, or causing another to commit perjury. The elements of Subornation of Perjury are:

a. That the accused induced and procured a certain person to take an oath or its equivalent and to falsely testify, depose, or state upon such oath or its equivalent concerning a certain matter;

b. That the oath or its equivalent was administrated to said person in a matter in which an oath or its equivalent was required or authorized by law;

c. That the oath or its equivalent was administered by a person having authority to do so;

d. That upon the oath or its equivalent said person willfully made or subscribed a certain statement;

e. That the statement was material;

f. That the statement was false;

g. That the accused and the said person did not then believe that the statement was true; and

h. That, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces or was of a nature to bring discredit upon the armed forces. "Induce and procure" means to influence, persuade, or cause.

33-3.15. Elements of False Swearing. The elements of false swearing under the UCMJ (Article 134) are as follows:

a. That the accused took an oath or equivalent;

b. That the oath or equivalent was administered to the accused in a matter in which such oath or equivalent was required or authorized by law;

c. That the oath or equivalent was administered by a person having authority to do so;

d. That upon this oath or equivalent the accused made or subscribed a certain statement;

e. That the statement was false;

f. That the accused did not then believe the statement to be true; and

g. That under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces or was of a nature to bring discredit upon the armed forces.

33-3.16. Legal Discussion – False Statements. False Swearing is the making under a lawful oath or equivalent of any false statement, oral or written, not believing the statement to be true. It does not include such statements made in a judicial proceeding or course of justice, as these are under Article 131, Perjury. Unlike a false official statement under Article 107, there is no requirement that the

statement be made with an intent to deceive or that the statement be official.

33-3.17. Elements of False Official Statement. The elements of a False Official Statement under the UCMJ (Article 107) are as follows:

a. That the accused signed a certain official document or made a certain official statement;

b. That the document or statement was false in certain particulars;

c. That the accused knew it to be false at the time of signing it or making it; and

d. That the false document or statement was made with the intent to deceive.

33-3.18. Legal Discussion – False Official Statements. This offense, which is somewhat related to perjury (although not involving an oath), is a violation of Article 107 of the UCMJ.

a. Official Documents and Statements. These include all documents and statements made in the line of duty.

b. Status of the Victim of the Deception. The rank of the individual intended to be deceived is immaterial, so long as that person was authorized or required to receive the statement or document from the accused. The government may be the victim in this situation.

c. Intent to Deceive. The false representation must be made with the intent to deceive. However, it is not necessary that the false statement be material to the issue of inquiry.

d. Knowledge that the Document or Statement is False. The false representation must be one, which the accused actually knew was false. Actual knowledge may be proved by circumstantial evidence. An honest, although erroneous, belief that a statement made is true, is a defense.

33-3.19. False Statement by Victims and Witnesses. A military member who is the victim of an alleged crime who makes a false report of a crime to a military authority (command personnel), military law enforcement (e.g., MP or CID), or an NCIS special agent may be convicted of making a false official statement in violation of Article 107, UCMJ. A civilian or military dependent who is the victim of an alleged crime who makes a false report of a crime to military law enforcement (while within their jurisdiction) or an NCIS special agent may be potentially violating Title 18 USC Section 1001 (False Official Statements).

33-3.20. Elements of Impersonation. The elements of Impersonating a Commissioned, Warrant, Noncommissioned, or Petty Officer, or an Agent or Official under the UCMJ (Article 134) are as follows:

a. That the accused impersonated a commissioned, warrant, noncommissioned, or petty officer, or an agent of superior authority of one of the armed forces of the United States, or an official of a certain government, in a certain manner; and

b. That the impersonation was wrongful and willful; and

c. That, under the circumstances, the conduct of the accused was to the prejudice of good order and discipline in the armed forces or was of a nature to bring discredit upon the armed forces.

NOTE 1: If intent to defraud is in issue, the following additional element is subsequent to "Element b." above: That the accused did so with the intent to defraud a certain person or organization in a certain manner.

NOTE 2: If the accused is charged with impersonating an official of a certain government without an intent to defraud, the following additional element is subsequent to 'Element b.' above: That the accused committed one or more acts which exercised or asserted the authority of the office the accused claimed to have.

33-3.21. Legal Discussion – Impersonation. Whoever falsely assumes or pretends to be an officer or employee acting under the authority of the United States or any department, agency or office thereof, and acts as such, or in such pretended character demands or obtains any money, paper, document, or thing of value is guilty of false personation.

a. Nature of Offense. Impersonation does not depend upon the accused deriving a benefit from the deception or upon some third party being misled, although this is an aggravating factor.

b. Willfulness. Willful means with the knowledge that one is falsely holding one's self out as such.

c. It must be proven that the person willfully, wrongfully, and publicly wore the uniform and insignia of a specific rank or impersonated an agent or official of the government by showing credentials or by otherwise misrepresenting himself for gain as outlined in the definition. The NCIS does not normally investigate matters where the impersonation was not executed for gain. In matters where the suspect's initial intent is unclear, an investigation may also be warranted.

33-3.22. Elements of Usury. The elements of Usury under the UCMJ (Article 92: Failure to Obey a Regulation or Order) are as follows:

a. No person in the Naval Service on active service, who makes a loan of money to another member of the armed services, shall knowingly charge, demand, or receive money or other property, constituting interest, in an amount or having a fair market value in excess of eighteen percent per year simple interest. Interest on such a loan for a period other than one year shall not exceed the equivalent simple interest rate for such period. (U.S. Navy Regulations, 1990, Article 1112)

b. Violations of Navy regulations are punishable under the UCMJ by up to two years in confinement. Simple usury cases are investigated by NCIS as violations of Article 92 (Failure to Obey a Regulation or Order) of the UCMJ. If the elements of aggravated assault, extortion and/or the communication of a threat are present, the investigation is to be conducted under that appropriate and relevant case category.

c. If NCIS conducts an investigation for usury, it should be investigated under the Special Inquiry category (7X).

33-3.23. Elements of Obstructing Justice. The elements of obstruction of justice under the UCMJ (Article 134) are as follows:

a. That the accused wrongfully did a certain act;

b. That the accused did so in the case of a certain person against whom the accused had reason to believe there were or would be criminal proceedings pending;

c. That the act was done with the intent to influence, impede, or otherwise obstruct the due administration of justice; and

d. That under the circumstances, conduct of the accused was to the prejudice of good order and discipline in the armed forces or was of a nature to bring discredit upon the armed forces.

33-3.24. Legal Discussion – Obstructing Justice. Obstructing justice may be based on conduct occurring before referral of charges. Actual obstruction of justice is not an element of this offense.

a. Criminal Proceedings. Include non-judicial punishment (NJP) proceedings under the Manual for Courts-Martial (MCM). Examples of obstruction of justice include:

(1) Wrongfully influencing, intimidating, impeding, or injuring a witness, a person acting on charges under the MCM, an investigating officer under Rules for Court Martial (RCM) 405, or a party, and

(2) By means of bribery, intimidation, misrepresentation, force or threat of force delaying or preventing communication of information relating to a violation of any criminal statute of the United States to a person authorized by a department, agency, or armed force of the United States to conduct or engage in investigations or prosecutions of such offenses; or endeavoring to do so.

b. If NCIS conducts an obstruction of justice investigation, it should be investigated under the 'Special Inquiry' category (7X).

33-3.25. Elements of a Hate Crime. The key element of a hate crime requires the offender's bias to be the <u>motivation</u> behind the criminal act. Issues to consider when determining whether an underlying crime can be associated with a hate crime are:

a. The offender and victim were of different race, religion, disability, sexual orientation, and/or ethnicity/national origin;

b. Bias-related oral comments, written statement or gestures were made by the offender, which indicate his bias;

c. Bias-related drawings, markings, symbol, or graffiti were left at the crime scene;

d. Certain objects, items or things that indicate bias were used;

e. The victim is a member or advocate of a racial, religious, disability, sexual orientation, and/or ethnic/national origin group;

f. The offender was previously involved in a similar hate crime or is a hate group member;

g. The area where the crime occurred is a known locale of high tensions between groups with a historically established animosity toward each other;

h. Several incidents occurred in the same locality, at or about the same time and the victims were all of the same race, religion, disability, sexual orientation, or ethnicity/national origin;

i. The victim was engaged in activities promoting his race, religion, disability, sexual orientation, or ethnicity/national origin;

j. The incident coincided with a holiday or a date of particular significance relating to a race, religion, disability, sexual orientation, or ethnicity/national origin; and

k. There are other indications that a hate group was involved (i.e., claimed responsibility).

33-3.26. Legal Discussion – Hate Crimes

a. A hate crime is a criminal offense that is motivated by the perpetrator's bias against the victim's race, color, religion, or national origin. Although the term "hate crime" is frequently used, the statute prohibiting them, 18 USC 245, provides a very narrow interpretation of what qualifies as a hate crime. Also, prosecution of a hate crime requires approval from the Attorney General, the Deputy Attorney General, the Associate Attorney General, or an Assistant Attorney General designated by the Attorney General to act in this capacity.

b. The UCMJ does not contain a prohibition on hate crimes per se. Within the DON, U.S. Navy Regulation 1167 prohibits supremacist activities that are commonly associated with hate crimes. NCIS does not normally investigative hate crimes as a separate, distinct offense under the UCMJ. Allegations of hate crimes should be investigated in accordance with recognized procedures for investigating the underlying or primary crime, such as assault, rape, homicide, or housebreaking. In addition to any other criminal charges stemming from an investigation, the convening authority could charge a suspect with violation of Article 92 of the UCMJ, failure to obey an order or regulation (U.S. Navy Regulation 1167), if evidence of supremacist activities or views are found during the investigation.

c. The RCM 1001 (b)(4) allows the presentation of evidence that the offender selected the victim based on "actual or perceived race, color, religion, national origin, ethnicity, gender, disability, or sexual orientation" during the pre-sentencing portion of a court-martial.

33-3.27. Elements of Stalking. The elements of stalking under the UCMJ (Article 120a) are as follows:

a. That the accused wrongfully engaged in a course of conduct directed at a specific person that would cause a reasonable person to fear death or bodily harm, including sexual assault, to him/herself or a member of his/her immediate family;

b. That the accused had knowledge, or should have had knowledge, that the specific person was placed in reasonable fear of death or bodily harm, including sexual assault, to him/herself or a member of his/her immediate family; and

c. That the acts induced reasonable fear in the specific person of death or bodily harm, including sexual assault, to him/herself or to a member of his/her immediate family.

33-3.28. Legal Discussion – Stalking

a. "Course of Conduct." This refers to a repeated maintenance of visual or physical proximity to a specific person or a repeated conveyance of verbal threat, written threats, or threats implied by conduct, or a combination of such threats, directed toward a specific person.

b. "Repeated." In reference to conduct, means two or more occasions of such conduct.

c. If NCIS investigates a stalking case, it should be investigated under the Special Inquiry (7X) category.

33-4. INVESTIGATIVE CONSIDERATIONS

33-4.1. Violence in the Workplace. Violence in the workplace is a continuing concern to supervisors and employees. Violence in the workplace can often result in the manifestation of a number of criminal acts including, but not limited to: assault, stalking, murder, robbery, bombings, arson, and threats. The purpose of this section is to assist field offices in providing guidance to commands responding to potentially violent situations.

33-4.2. A number of factors may contribute to violent behavior, including, but not limited to: personal relationship problems (e.g., marital conflicts, domestic abuse, child custody issues, etc.), substance abuse, incapacity to resolve personal problems, and/or workplace conflicts with supervisors and/or co-workers. Some of these behaviors may become criminal or may have the potential for escalation. The behaviors may include intimidation, harassment, verbal abuse, assault, or use of a weapon.

33-4.3. Proactive awareness of the signs for violent behavior is key to the prevention of potentially violent escalations in the workplace. Threat Management Unit (TMU) field office representatives and/or the TMU NCISHQ should be contacted for guidance when workplace violence is suspected. TMU can provide a risk/violence assessment and evaluation.

33-4.4. Employers are responsible for ensuring a safe work environment for all employees.

Furthermore, employers should develop effective communication and listening skills, provide clear guidance on unacceptable types of workplace behavior, and document all unacceptable behaviors and actions taken.

33-4.5. Careful analysis of a situation must first be conducted upon notification of a potentially dangerous workplace incident involving an employee or service member. If the individual(s) exhibits behavior involving intimidation, harassment, bizarre or irrational acts, appears intoxicated or impaired, and/or poses a potential threat to employees or self but has neither presented, announced a threat, nor committed a criminal act, the following courses of action are suggested to the command.

a. Consideration should be given regarding consulting/interviewing representatives from professional groups to include: human resources, Employee Assistance Program (EAP) coordinators, family services, counseling and medical professionals, security, law enforcement, and legal.

b. Determine whether previous warnings were given to the employee regarding inappropriate and intolerable behavior. Counseling should be provided by the command to offer assistance and appropriate referrals.

c. Refer to EAP or medical counsel if issues are raised regarding mental or physical health. Obtain a waiver from the individual prior to the referral in order that command and/or NCIS may access records.

d. Through discussions with Human Resources, determine if disciplinary action is viable or alternative solutions may better accommodate the employee. (Note that reasonable accommodation may be a requirement in accordance with the Americans With Disabilities Act of 1990.)

e. Grant an excused absence, if necessary or appropriate.

33-4.6. Threat Management Unit (TMU). A significant number of criminal investigations involve workplace violence, stalking, juvenile violence, serial crimes, and threatening communications. In response, the TMU was established to provide criminal and behavioral analysis and risk assessments for the potential for violence. Investigative analysis includes risk assessments, interview and interrogation strategies, and approach techniques and strategies. The TMU consists of special agents, staff psychologists, analysts, and others as deemed appropriate.

33-4.7. In unknown subject(s) investigations, the TMU can provide assessments of potential suspect(s). The TMU is available to provide specific and individual guidance on any investigation deemed appropriate. These often include, but are not limited to: threatening communications, stalking, serial crimes, juvenile violence, self-mutilation, hate crimes, and workplace violence. Case agents should contact their local TMU field representative or the TMU NCISHQ Program Manager to coordinate and discuss the specific aspects of the investigation.

NOTE: Any documentation provided to the case agent from TMU is to be utilized by the case agent as “case notes” and may not be attached to any external reports without TMU approval. The

information provided by TMU can be used to verbally brief commands and other concerned parties.

33-4.8. The TMU has developed an interview protocol to assist the field agent with interviewing/interrogating; this information can be provided by the TMU upon request.

33-4.9. The TMU maintains a security checklist, which provides guidance and suggestions for victim safety. This checklist can also be found on the NCIS Infoweb.

33-4.10. The TMU maintains a database of unsolicited communications. This database includes communicated and/or potential threats. All unsolicited communications should be forwarded to the TMU NCISHQ 23B1 for inclusion in the database. Information regarding a specific communication or an individual is available through the TMU.

33-4.11. Threats of violence (to include workplace violence, stalking, property damage, etc.) to agents, DON personnel, and their families are to be addressed immediately. The TMU will respond to requests for guidance regarding threat assessment and threat management on a real time basis. To facilitate a timely and comprehensive assessment, photocopies of all case information, correspondence, audiotapes, videotapes, transcriptions, and other pertinent information must be forwarded to the TMU representative as expeditiously as possible.

33-4.12. Family Advocacy Program (FAP)

a. SECNAVINST 1752.3B (10NOV05), "Family Advocacy Program (FAP)," establishes a policy on family advocacy within the DON and assigns responsibilities for the FAP. FAP is responsible for addressing the prevention, evaluation, identification, intervention, treatment, follow-up, and reporting of child and spouse maltreatment, sexual assault, and rape. OPNAVINST 1752.2A (17JUL96), "Family Advocacy Program," directs all DON personnel to report any incident or suspected incident of child abuse occurring on a military installation or involving persons eligible for FAP services to the local Family Advocacy Representative (FAR). The FAR will notify the member's command and appropriate state and civilian agencies having a protective service function (e.g., Child Protective Services). Agents are responsible for becoming familiar with local child protective agencies and resources. In cases of major physical injury, the FAR will also notify the appropriate law enforcement personnel. To ensure NCIS jurisdictional responsibilities under the FAP are met, each NCIS field component should accomplish the following on a continuing basis:

(1) Maintain liaison with the Commanding Officer of the Military Treatment Facility in the NCIS area of jurisdiction to ensure the local lines of communication are open and the FAR and medical personnel are aware of their responsibility to immediately notify NCIS of cases involving suspected or actual child abuse and criminal forms of child neglect.

(2) Advise the FAR and indicated medical representatives of NCIS investigations to be conducted for criminal acts within permissions by reason of jurisdiction over the person(s), place(s), or offense(s) involved. NCIS may also coordinate the matter with other authorities for investigation.

(3) In a case initiated by NCIS that was not based upon notification by DON medical

authorities and involves a military member (whether deemed a suspect or victim), the local NCIS office should apprise the FAR of the open investigation and provide pertinent data relative to the criminal offense.

33-4.13. Reporting Requirements for Health Care Providers. Title 42 USC Section 13031 mandates health care professionals, who provide services on federal land or in a federally operated facility, report child abuse to the local law enforcement agency that has jurisdiction to investigate such abuse. Healthcare professionals include physicians, dentists, residents hospital personnel, nurses, pharmacists, emergency medical technicians and "persons performing a healing role or practicing the healing arts." Under SECNAVINST 5430.107, NCIS has primary responsibility for investigating felonies in naval treatment facilities. Thus, healthcare professionals at naval treatment facilities should report all suspected child abuse cases directly to NCIS. Detailed and timely reporting is mandatory in all cases investigated. The commanding officer of the appropriate Naval Hospital should be notified when another medical authority or investigative agency seeks investigative assistance. Documentation of the request or notification should be included in a report of investigation. Failure to report is a federal crime under 18 USC 2258.

33-4.14. Traffic Accident Investigations. The "Traffic Accident" case subcategory (7T) is used for investigations regarding the unlawful departure from the scene of an accident without rendering assistance to the injured or making identity known. This subcategory may also include incidents involving the collision of motor vehicles, vehicular damage to government or personal property, and vehicular injury to pedestrians. See section 33-2.2 above in relation to NCIS policy regarding vehicular fatalities.

a. SECNAVINST 5430.107 provides that the investigation of minor offenses shall be completed by command investigators within the Navy and Marine Corps (masters-at-arms, base police, Marine CID, etc.). A traffic accident may be either a major or minor offense, or the traffic accident may not necessarily constitute any offense against the UCMJ, statutes, or regulations. Investigation of accidents involving motor vehicles normally shall be conducted by the affected military command, such as a Preliminary Investigation or JAGMAN Investigation. However, NCIS field components may from time to time render specialized investigative services to military commands who have undertaken the investigation of a traffic accident. This request for assistance may take the form of a request to render the following services:

(1) Interview of witnesses or interrogation of suspects;

(2) Polygraph services;

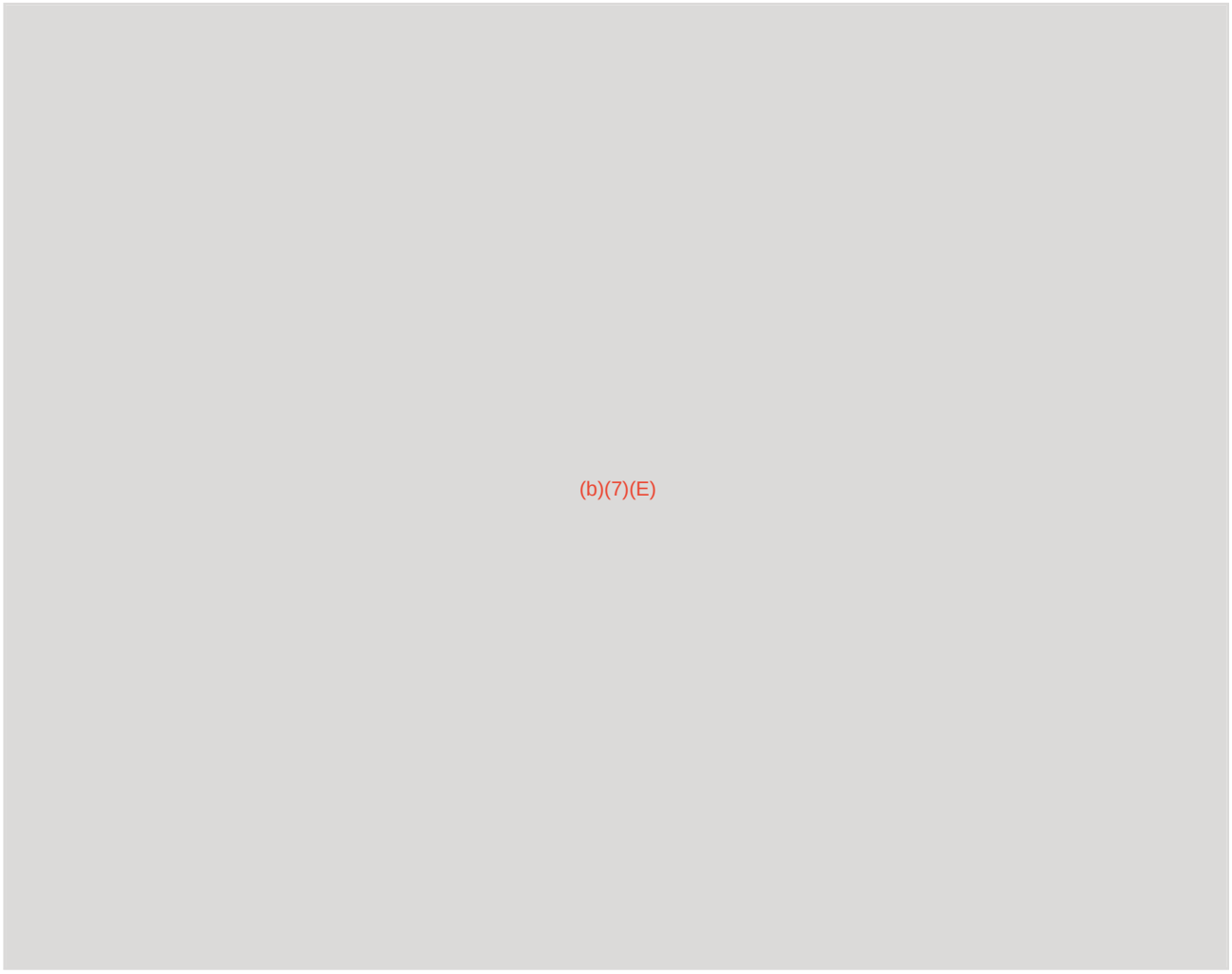
(3) Fingerprinting services; and

(4) Laboratory analysis of physical evidence.

b. On occasion, a military command may request NCIS to participate in the investigation of a traffic accident involving military personnel occurring off the installation. This type of investigation is initiated by the military command to make an "in the line of duty" determination where civilian law enforcement authorities may have conducted the investigation of the traffic

accident. Cases of investigative assistance rendered to the military command in this regard by NCIS should be assigned to this category (7T).

c. The investigation of vehicular traffic accidents should not normally be undertaken by NCIS. The request for investigative assistance should contain an element of urgency, aggravation, or specialization within the meaning of this subcategory (7T).



33-4.16. Unlawful Dissident and Protest Activities. The investigation of DoD affiliated personnel involved in "Unlawful Dissident and Protest Activities," as set forth below, should be investigated under the subcategory of Special Inquiry (7X). Activities that can be investigated under this subcategory include:

a. Direct or indirect affiliation or association with, or membership in organizations or groups, which advocate alteration of the form of government of the United States by unconstitutional means.

b. Advocating the denial of the Constitutional rights of others. This includes direct or indirect affiliation or association with or membership in organizations or groups which advocate denial of

the constitutional rights of others.

c. Attempts to undermine the loyalty, morale, good order and discipline, and operations of the Navy or Marine Corps by actively encouraging violation of law, disobedience of lawful order or regulation, or disruption of military activities.

d. Dissident or protest activities in violation of lawful orders or regulations.

33-4.17. Legal Discussion – Unlawful Dissident and Protest Activities. The investigation of the activities described in the above circumstances, which lack a substantive connection to foreign powers, persons, or groups, do not meet the definition of counterintelligence provided in Executive Order (EO) 12333, "US Intelligence Activities." Investigations in this subcategory are undertaken as a law enforcement function to investigate suspected violations of federal law (including the UCMJ) and DoD and DON orders and regulations. Investigations under this subcategory are also initiated as a preventative law enforcement function to determine if the activities of DoD affiliated persons pose a threat to DON personnel, equipment, installations, or operations.

The legal authority and guidelines applicable to dissident and protest activities among military members of the Armed Forces are set forth in DoD Directive 1325.6, “Guidelines for Handling Dissident and Protest Activities Among Members of the Armed Forces.” OPNAVINST 1620.1B and MCO 5370.4B reiterate the DoD Directive to the USN and USMC for information and compliance. The substance of DoD Directive 1325.6 is as follows:

a. Active Participation

(1) Members of the armed forces are expressly prohibited from active participation in organizations which:

(a) Espouse supremacist causes,

(b) Attempt to create discrimination,

(c) Advocate the use of force or violence, or

(d) Otherwise deny civil rights.

(2) Active Participation includes demonstrating, rallying, fund raising, recruiting, training, or leading. It does not include membership or mere presence at an event. Commanders are authorized to take administrative and disciplinary action against offenders.

b. Possession and Distribution of Printed Material

(1) A commander may require prior approval be obtained for distribution of a publication on an installation in order to determine if there is a clear danger to good order and discipline. A commander may not prohibit the distribution of a specific issue of a publication distributed through official outlets such as base exchanges and military libraries.

(2) Mere possession of unauthorized printed material may not be prohibited, but such material may be impounded if the commander determines distribution will be attempted.

(3) The fact that a publication is critical of government policies or officials is not, in itself, sufficient to prohibit distribution.

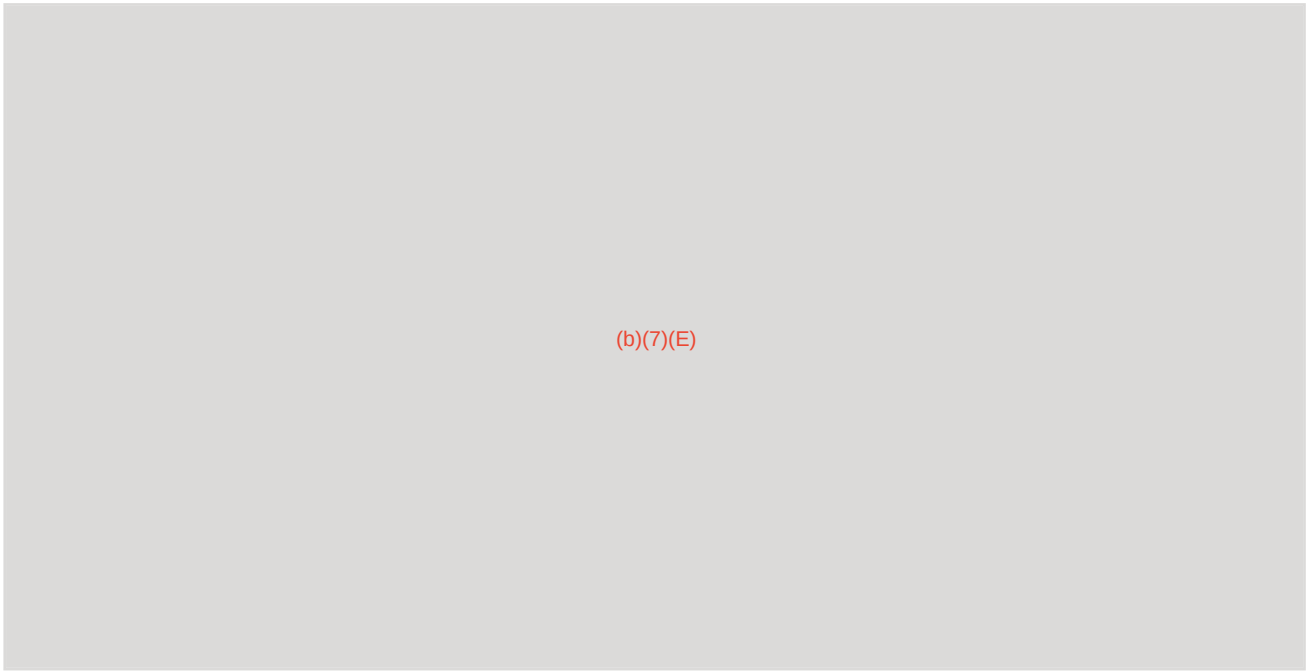
c. Off-Post Gathering Places. If activities taking place in an off-post gathering place include counseling members to refuse to perform duty, to desert, or to disobey direct orders, the commanding officer may place such an establishment "Off Limits" in accordance with established procedures.

d. Underground Newspapers. When a publication is either written during duty hours, on government property, or contains language urging actions punishable under Federal law, those involved in its publication may be disciplined for the infraction and such publications may be prohibited.

e. On-Post Demonstrations and Similar Activities. Any activity on an installation which could result in interference of orderly accomplishment of the mission of the installation or presents a clear danger to the loyalty, discipline, or morale of the troops may be prohibited. (See 18 USC 1382.)

f. Off-Post Demonstrations. Members of the armed forces are prohibited from participating in unauthorized off-post demonstrations when they are on duty, or in a foreign country, or when their activities constitute a breach of law and order, or when they are in uniform, or when violence is likely to result.

33-5. INVESTIGATIVE PROCEDURES



e. Interrogation of the suspect should generally be attempted only after other investigative procedures have been employed. Ensuring the safety of the victim is imperative, particularly once the suspect(s) becomes aware that the extortion attempt has been uncovered.

f. It is important that the language of any oral threat communicated be ascertained in as near verbatim language as possible. Attempt to resolve any apparent conflict in witness statement(s), without actually compromising or influencing the statement's intended meaning. Clarification for why any communicated words were regarded as threatening is vital.

g. Any assistance necessary to the victim should be ensured when efforts are being made to articulate the fear and receipt of a threat and should be reflected in the victim's statement.

h. In conducting any extortion investigation, ascertain and document the value of all items extorted.

i. Photograph all subjects for inclusion into the TMU database.

33-5.2. Investigative Procedures - Kidnapping. The following are investigative steps to consider in response to a kidnapping situation.

a. Interview complainants, witnesses, parents, friends, neighbors, and co-workers in an effort to obtain as much information as possible concerning the subject(s) and victim(s), key words and/or phrases used, description(s) (including clothing), pictures, mental state, habits, etc.

b. Establish modus operandi of suspects.

c. Consider the use of immediate hypnotic interviews of witnesses, if appropriate.

d. Compile a complete description of suspects, their vehicles, weapons, etc.

e. If suspects are known, develop background information, including police background checks (e.g., NLETS, etc).

f. Establish a base of operations in or near the crime scene (point where suspect(s) may attempt to contact loved ones of the victim). Establish a "think tank" to explore all options. Ensure compatibility of communications with other agencies, recruit interpreters if necessary.

g. Ensure careful collection and handling of written letters or messages from suspect(s), as to preserve item(s) for processing as evidence.

h. Note background noises, voice characteristics, accent, and exact words used (record if possible) when documenting verbal contact with suspects.

i. Immediately obtain permission for use of wiretap/eavesdrop equipment as necessary.

j. Assist in marking/recording money for future tracing of ransom payment, if necessary.

k. Coordinate the pre-positioning of an arrest/apprehension team. Contact the TMU, NCISHQ, Code 23B. If in the United States, coordinate with the FBI and/or state authorities as appropriate. If overseas, coordinate investigation with local authorities per Status of Forces Agreement, as appropriate.

33-5.3. Investigative Procedures – Child Abuse. The following are investigative steps to consider in response to a child abuse allegation.

a. All NCIS investigations regarding child abuse, which are not sex related, and child neglect matters are conducted under Category 7L. Investigations involving sexual abuse of a child are conducted under Category 8B, Sex Abuse-Child (see NCIS-3, Chapter 34). Successful completion of these investigations requires a coordination of the investigative skills of the agent with those of the medical profession and/or forensic consultant. It is especially important the agent maintain close liaison with the appropriate FAP/FAR (for family advocacy record checks) and hospital representatives who can assist in providing professional medical expertise, medical records, interpretation of X-rays, and medical reports, as well as access to other medical personnel for interviews. The Armed Forces Center for Child Protection, located at the National Naval Medical Center, Bethesda, MD, is also an excellent resource for child abuse investigations, providing a full array of medical exams, forensic interviews, or expert consultations for more difficult cases.

b. Investigations of child abuse and child neglect matters should generally begin with the interview of the person(s) apprising NCIS of the incident. In many instances, the complainant will be either the local FAR or other medical professional at the hospital.

c. The investigation should document the following basic information:

(1) What is the nature of the abuse? Is it sexual?

(2) Did the complainant witness the assault, and what is the basis of the allegation of child abuse?

(3) Was the child hit, punched, slapped, or was some type of weapon used to inflict the assault?

(4) Was there an offer to do harm or an attempt to injure? Was the child merely threatened or scolded?

(5) When and where did the abuse occur? How many times?

(6) What was the character and extent of the injury?

(7) What is the nature of the husband/wife relationship, and what is the general attitude of the parent(s) toward the child/victim and other children?

(8) Did the child receive medical attention?

(9) If the complainant is an adult (parent, neighbor, command representative, etc.), will the complainant be willing to furnish a written statement regarding knowledge of the matter?

d. Early in the investigation, agents should request from military medical treatment facilities the pertinent medical records. If possible, parental consent should be acquired via a signed Health Insurance Portability and Accountability Act (HIPAA) form. In most instances, medical authorities will ensure the victim will be afforded a thorough medical examination. The investigating agent should effect liaison with the appropriate medical authorities to ensure the medical examination includes the following:

(1) Full body X-rays to document:

(a) Long bone fractures/injuries, which are either new or in a state of healing;

(b) Excessive new long bone formation;

(c) Multiple bone fractures/injuries;

(d) Separation/twisting of the joints;

(e) Periosteal hematoma and calcification of the joints; and

(f) Head injuries (subdural hematoma).

(2) Full body examination to document soft tissue injuries such as contusions, burns, abrasions, and other visible marks on the exterior of the victim's body. The examination should also include a search for any injury, which may indicate the pattern of the weapon that inflicted the injury (e.g., a belt, belt buckle). The medical examination should further look for signs the victim suffers from a pre-existing medical condition (such as brittle bone disease), which may account for the injury. Furthermore, a thorough examination of siblings for signs of abuse must be considered in all cases.

(3) Examination for indications of sexual abuse, which often accompanies physical abuse.

e. In addition to the examination of the child to detect physical abuse, observations to detect signs of neglect should be documented and include:

(1) Height and weight of the child to determine if they are within normal limits for the age;

(2) General state of nutrition;

(3) General condition (e.g., cleanliness of the child and clothing worn); or

(4) Presence of severe diaper rash, skin infections, or similar ailments.

f. The investigating agent should ensure copies of all photographs are obtained and incorporated into investigative documentation. Because contusions may become more apparent following the initial examination, it is suggested additional requests for photography be made at a time when the contusions are determined by medical authorities to be at their peak. All physical injuries should be documented by color photography. The investigating agent should ensure all photographs are provided to NCIS along with copies included in the medical record of the victim. When it is necessary that a NCIS agent accomplish photography, it should be done with the assistance of a medical professional.

g. Early in the investigation, the parents or guardian of the victim should be interviewed. Parents are also potential suspect(s) and may be responsible for the abuse or neglect directed against the child. In cases where parent(s) or guardian(s) are suspect, or when that person begins to make incriminating statements during the initial interview, the investigating agent must apprise the person of his or her rights pursuant to the UCMJ if the parent or guardian is subject to the code. A Miranda Warning is to be given to non-military personnel if in a custodial setting.

h. The investigation should routinely include interviews of all individuals who may be knowledgeable of pertinent information. Those persons may include, but are not limited to:

(1) Neighbors;

(2) Family friends;

(3) Work associates;

(4) Medical personnel;

(5) Babysitters;

(6) Child care center or school personnel; or

(7) Other children of the approximate age of the victim (when appropriate).

i. When the victim is of an age that will allow for a meaningful interview, the interview should be conducted in concurrence with medical professionals or those trained in child forensic interviewing. Interviews of juveniles must be done with the consent of a parent or, when appropriate, by legal authority.

j. In addition to the review of pertinent medical records and interviews of knowledgeable individuals, an examination of the scene where the physical abuse or neglect occurred should be accomplished. In many instances, examination of the victim may reveal a patterned injury made by such instruments as belts, belt buckles, hairbrushes, wire, cords, and other instruments that leave a unique pattern on the skin of the victim. During a search, instruments that have inflicted such injuries may be observed. Such instrument(s) should be seized under existing NCIS evidence handling procedures. In cases of neglect, examination of the family residence may reveal unkempt living conditions. Full photographic coverage of the scene (color photography) is essential to

adequately document the scene.

k. Immersion Burns. During an investigation involving immersion burns (i.e., burns resulting from immersion in hot water/bathtub), a crime scene examination should be completed to document the size, style, construction, etc, of the bathtub or washbasin and the water heater involved. The water heater should be examined to determine if it is operating properly. This requires the temperature readings to be taken at various times and at various depths by two agents with two different thermometers capable of recording water temperatures up to 212 degrees Fahrenheit or 100 degrees Celsius. The temperature setting of the water heater should be recorded at both thermostats. To assist with investigations involving immersion burn injuries, Appendix (1), Evidence Worksheet for Immersion Burns, should be completed.

33-5.4. Investigative Procedures – False Official Statements, Perjury and False Swearing. The following are investigative steps to consider in response to a false official statement, false swearing or perjury situation. A Perjury will occur during a judicial proceeding (i.e., in court), while a false official statement or false swearing does not occur during a judicial proceeding.

When an agent determines the victim in a case made a false complaint or the investigation indicates suspicion of a false complaint, the victim will be appropriately warned. If an admission is obtained from the victim or enough evidence exists to implicate him in a false complaint, the investigation will be terminated. The decision to prosecute a case or take disciplinary action is the responsibility of command and legal authority (e.g., SJA, AUSA, or DAO). If command determines there is insufficient evidence to prosecute a case, the report should indicate the case was presented to command and command declined to prosecute to due to lack of evidence, victim recantation, etc. If a victim recants and states they lied about the allegations, the case should be closed and the victim will remain in the victim title block. A Perjury (7P) investigation will then be initiated, indexing the former victim as a subject in the NI title block. It is important to reference the first investigation and clearly articulate why the Perjury (7P) investigation was initiated.

a. Reporting Requirements. The following will be addressed in the reports of the investigation:

(1) All investigative effort expended to address the allegation; and,

(2) Why the investigation was closed prior to completion of all proper investigative leads; and,

(3) Information developed during the investigation which supports the evidence of a false complaint; and

(4) That subject notification was effected.

b. Procedures. The investigative procedures to be followed in perjury, false swearing, and false official statements cases will be suggested by the circumstances of the particular case. The challenge will be to collect information of evidentiary value that the accused did not believe the statement to be true at the time he allegedly perjured himself or made the false statements. As in most matters involving knowledge, intent, or belief, it is usually possible that only reasonable inferences be drawn from surrounding circumstances. Agents should not assume the victim in a

case is lying when the victim may simply be recalling additional information. A false complaint is when the victim deliberately fabricates an allegation that a crime has occurred.

33-5.5. Investigative Procedures - Impersonation. The following are investigative steps to consider in response to an impersonation allegation.

a. Establish the willful and illegal wearing of a uniform or the impersonation of an officer or enlisted person of the U.S. military for gain as outlined above in the Elements of the Crime.

b. When it is reported that an active or reserve duty military member is carrying on an impersonation and an investigation is requested, the NCIS special agent should interview the original reporting individual, documenting such information as when and where the impersonation occurred and its frequency. The investigating agent should ascertain how the original informant identified the individual, and any rationale or insight for the performance of the impersonation (e.g., to perpetrate fraud, sexual advances, etc.).

c. The investigation should further attempt to establish a pattern of activity by documenting the suspect's movements. Following this, surveillance arrangements should be made so that the suspect's movements can be monitored over a period of time, enabling a clear determination to be made as to whether an impersonation is being executed. Photography should be used as an investigative aid and statements should be obtained from all persons approached by the suspect, detailing all encounters and describing the extent of the impersonation.

d. If it is reported that an individual (civilian or military) is impersonating an officer or employee acting under the authority of the U.S. or any department, agency or officer thereof and demands or obtains money, papers, documents or anything of value, may be in violation of Title 18 USC 912 (False Personation). If the suspect, while under the false personation, arrests or detains any person or in any manner searches the person, buildings, or other property of any person, may be in violation of Title 18 USC 913 (Impersonator Making False Arrest or Search).

(1) EXAMPLE 1: An enlisted person impersonating an NCIS special agent to falsely detain a person for a driving violation is potentially violating either Article 134 of the UCMJ or Title 18 USC 913.

(2) EXAMPLE 2: A civilian impersonates a Marine Corps officer and attempts to acquire a CAC card to gain access to a military installation, may be violating Title 18 USC 912.

33-5.6. Investigative Procedures – Unlawful Dissident Activities. The following are investigative steps to consider in response to allegations of unlawful dissident and protest activities.

a. A careful evaluation of the initial allegation, complaint or intelligence received must be made prior to the initiation of an investigation. An investigation is initiated only if the information raises a reasonable suspicion that the person violated federal law or DoD/DON regulation or that the person has shown a proclivity to engage in activity which would threaten DON personnel, equipment, installations or operations. The narrative paragraph of the ROI will clearly identify the purpose of the investigation. The following are samples of possible narrative paragraphs.

(1) Law Enforcement Investigation.

“On (date), the Commanding Officer, (Command), advised that allegations had been received that subject and co-subject are actively recruiting members for (organization name) aboard the installation in violation of (cite law or applicable regulation).”

(2) Preventative Law Enforcement Investigation.

“On (date), a confidential source reported that subject and co-subject are members of an extremist organization, alleged by (FBI, local law enforcement, etc.) to have perpetrated violence in other areas. Subject and co-subject are believed knowledgeable of this penchant for violence and supportive of its use to achieve the organizations objectives.”

(3) Preventative Law Enforcement Investigation.

“On (date), information was received through a National Agency check that subject's father is a functionary of a radical revolutionary group and that subject is supportive of the illegal tactics and objectives of this group. Inquiries will be conducted to determine degree of contact, degree of influence, and subject's own involvement in the group's activity. Coordination with FBI has been conducted.”

b. Occasions will arise when "underground newspapers," dissident slogans, protest posters, etc., will appear aboard an installation with no apparent indication concerning the identity of the culprits. In such instances, investigations may be initiated to determine if an offense has occurred and the identification of likely suspects. In such cases the subject of the investigation should be the name of the installation followed by the type of activity. The subject of the case should not be the name of a civilian organization.

EXAMPLE: I/NAS JACKSONVILLE, FL/APPEARANCE OF DISSIDENT NEWSPAPERS ABOARD INSTALLATION

c. If the investigation develops that a crime has been committed and the persons responsible are civilians, the matter should be referred to the FBI. If the FBI declines the investigation, NCIS can investigate such activities by persons aboard base. NCIS cannot pursue off-base activities of civilians unless a crime has been committed and the investigation is fully coordinated with the FBI and/or any federal or local agencies having concurrent jurisdiction.

d. Investigative Techniques. Experience has shown that arbitrary background inquiries (i.e. references, employment, education, etc.) have generally been unproductive in resolving specific allegations. An in-depth review of the subject's service record should be conducted to determine, among other things, his level of security clearance, and exact nature of access. Also determine if the subject listed any organizational affiliations on statements of personal history, enlistment papers, or beneficiary papers.

(b)(7)(E)

Pages 1006 through 1010 redacted for the following reasons:
- -
(b)(7)(E)

NCIS-3, Chapter 34
Sex Offenses (Category 8)
Effective Date: October 2014

TABLE OF CONTENTS: **PAGE**

34-1. Purpose. Naval Criminal Investigative Service (NCIS) has the responsibility to conduct investigations of major criminal offenses within the Department of the Navy (DON), to include all reported incidents of sexual assault. The NCIS-3 manual, including this chapter, exists solely for internal agency guidance. This chapter does not place any limitations on otherwise lawful activities of the agency. References are listed in Appendix A. Abbreviations and acronyms frequently used during the investigation of sexual assaults are listed in Appendix B. Proper definitions and preferred terms to be used in documenting sexual assault investigations are provided in Appendix C.

34-2. Policy. NCIS personnel will follow DoD and DON policy regarding reports and investigations of sex offenses. Investigators should note the following references in particular:

a. Reference (a) mandates that military criminal investigative organizations (MCIOs) initiate investigations of all reported allegations of adult sexual assault, abusive sexual contact, and attempts, of which they become aware, that occur within their jurisdiction regardless of the severity of the allegation. NCIS sexual assault investigations will be timely, thorough, and comply with reference (a). NCIS shall initiate separate investigations if additional allegations of criminal activity against the victim (threats, minor physical assaults, damage to property, etc.) are identified during the investigation. NCIS will investigate all reports of adult sexual assault without regard to the known or assumed sexual orientation of the victims or subjects. Sexual orientation of victims, subjects, or anyone else associated with the case will not be documented in the investigation unless such details are specifically pertinent to the case. The primary NCIS agent or investigator assigned to conduct the sexual assault investigation must be properly trained in conducting such investigations. At a minimum, this training must include training specified in reference (a).

b. Reference (b) mandates that DoD components conduct sexual assault investigations, provide victim support services, have a 24/7 response capability, and complete specialized training. It describes restricted reporting, an option available for victims to facilitate services. MCIOs should not become aware of restricted reports; MCIOs' investigations result from unrestricted reports only. Additionally, reference (b) mandates that sexual assault response coordinators (SARCs) must enter all sexual assaults into the Defense Sexual Assault Incident Database (DSAID); enclosure (7) requires SARCs to convene a monthly multidisciplinary sexual assault case management group (SACMG) to review cases, facilitate monthly victim updates, and ensure system coordination, accountability, and victim access to quality services.

c. Pursuant to reference (c), which provides detailed requirements for DON components to comply with DoD mandates, NCIS Code 23C will collect all data according to DoD annual reporting requirements and submit all data in coordination with Service inputs from the Navy and Marine Corps. Additionally, in adult sexual assault cases controlled by NCIS, metrics regarding the time elapsed between initiation and pending prosecution will collected. Findings will be reported at least annually to the Secretary of the Navy via the DON Sexual Assault Prevention and Response Office. Reference (d) establishes the special victim capability within the MCIOs. For NCIS procedures for cases involving adult victims, see Appendix D. For special considerations for cases involving child victims, see Appendix E.

d. Pursuant to references (e) and (f), see Appendix F for policy on the Family Advocacy Program.

e. For policy regarding sex offender registration, see Appendix G.

34-3. Cancellation. NCIS-3, Chapter 34, dated September 2007; Gen Admin 11C-0018 of 7 June 2011, NCIS Policy Document No. 11-09 Operational (Additional Procedures to Child Pornography Investigations); and Gen Admin 11C-0028 of 7 October 2013, NCIS Policy Document No. 13-06 Operational (Investigation of Adult Sexual Assaults).

34-4. Chapter Sponsor. Criminal Investigation and Operations Department, Code 23B.

34-5. Criminal Law and Jurisdiction

a. Uniform Code of Military Justice (UCMJ). NCIS category "8" crimes are potential violations of the UCMJ Article 120 (Rape, sexual assault, and other sexual misconduct), Article 125 (Sodomy), and Article 134 (General Article). Regardless of where the offense occurs, NCIS maintains jurisdiction over all DON Service members, as they are subject to the UCMJ at all times. A major revision to Article 120 took effect June 28, 2012; earlier law applies to conduct before that date. The changes in 2012 expanded definitions of sexual act and sexual contact, modified definition of force, modified definition of consent, and restructured the offense categories of adult crimes (Article 120), stalking (Article 120a), child sexual assault (Article 120b), and other sexual misconduct (Article 120c). Also, child pornography is now specifically listed within Article 134. The descriptions and the definitions in Appendix C are based on the current UCMJ. For offenses committed before June 28, 2012, consult with the NCIS Legal Directorate and local staff judge advocates (SJAs) or prosecutors.

(1) Sexual act vs. contact. Understanding the differences between a sexual act (a penetration crime) and sexual contact (a touching crime) is key to understanding Article 120 and 120b offenses. Previously, a sexual act was limited to penetration of either the vulva or the genital opening. The 2012 revision expands "sexual act" to include penetration of the vulva or anus or mouth, in one of two ways: If a penis is involved, no specific intent is necessary. If the sexual act involves penetration by any other part of the body or by any object, the specific intent must be "to abuse, humiliate, harass, or degrade any person or to arouse or gratify the sexual desire of any person." The applicable offenses involving a sexual act are Rape and Sexual Assault, depending on degree of force involved.

(2) Expanded definition of contact. "Sexual contact" was expanded during the 2012 revision in two ways. The first added the phrase "causing another person to touch" to the 2007 definition, and the second included touching any body part for sexual gratification. The applicable offenses involving a sexual contact are aggravated sexual contact and abusive sexual contact. This expansion of "sexual act" and "sexual contact" will impact investigations of criminal behavior during hazing incidents.

(3) Force. Force is a key factor of Article 120. The 2012 version focuses on the offender's acts. "Force" includes both use of a weapon and use of physical strength or violence measured by an objective "reasonable person" standard to determine if the action is sufficient to overcome, restrain, or injure. Alternately, it also includes infliction of physical harm sufficient to coerce or compel submission. This anticipates a subjectively "vulnerable victim." Fact finders would look at all circumstances, including senior-subordinate status or disability, which would make a victim more easily coerced than the average person. The degree of force, threat, induced belief, or incapacitation used during the commission of a sexual act or sexual contact determines the applicable offense. For example, a high degree of force typically meets the elements of rape or aggravated sexual contact, while a lower degree of force would meet the elements of sexual assault or abusive sexual contact.

(4) Consent. Consent is a key factor of Article 120. The 2007 version made a sexual act illegal if the victim was "substantially incapacitated" or "substantially incapable" of appraising the nature of the sexual act. The 2012 version criminalizes commission of a sexual act upon another when the offender "knows or reasonably should know that the other person is asleep, unconscious, or otherwise unaware that the sexual act is occurring."

(5) Sodomy. Article 125 was amended in 2013 to remove consensual sodomy as an offense. Article 125 remains in effect for forcible sodomy and bestiality.

(6) Actual vs. "virtual" child pornography. Child pornography under Article 134 includes both images involving actual children and obscene "virtual" images, which do not depict actual children. Investigators should note that virtual child pornography will raise constitutional free speech concerns in relation to Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002). Accordingly, as with all Article 134 offenses, investigators should seek evidence that shows conduct "was to the prejudice of good order and discipline in the armed forces or was of a nature to bring discredit upon the armed forces."

(7) Mistake of fact and apparent age of child victims. Under Article 120b, individuals accused of child sex offenses may offer affirmative defense evidence of mistake of age for victims younger than 16 years, but not younger than 12 years.

(8) Statute of Limitations. There is no statute of limitations for rape or sexual assault, under Article 43 of the UCMJ. The usual 5-year UCMJ statute of limitations is extended to the life of the child victim in certain child sex offenses.

b. United States Codes

(1) The following sections of the United States Code (U.S.C.) are applicable to sexual offenses. Additional sections may apply.

Sections of Title 18 U.S.C. applicable to sexual offenses	
Section	Title
1384	Prostitution near military and naval establishments
1460	Possession with intent to sell, and sale, of obscene matter on federal property
1461	Mailing obscene or crime-inciting matter
1462	Importation or transportation of obscene matters
1463	Mailing indecent matter on wrappers or envelopes
1464	Broadcasting obscene language
1465	Transportation of obscene matters for sale or distribution
1466	Engaging in the business of selling or transferring obscene matter
1468	Distributing obscene material by cable or subscription television
1470	Transfer of obscene material to minors
2241	Aggravated sexual abuse (rape or child sexual assault)
2242	Sexual abuse
2243	Sexual abuse of a minor
2244	Abusive sexual contact
2245	Sexual abuse (rape or child sexual assault)
2246	Definitions of “sexual act” and “sexual contact” under the U.S.C.
2247	Repeat offenders (rape or child sexual assault)
2251	Sexual exploitation of children
2251A	Selling or buying of children
2252	Certain activities relating to material involving the sexual exploitation of minors
2252A	Certain activities relating to material constituting or containing child pornography
2258	Failure to report child abuse
2260	Production of sexually explicit depictions of a minor for importation into the United States
2425	Use of interstate facilities to transmit information about a minor
116	Female genital mutilation
Section of Title 47 U.S.C applicable to sexual assault offenses	
231	Restriction of access by minors to obscenity over the Internet

(2) For child pornography offenses committed before January 12, 2012, there is no specific UCMJ charge, but sections of the U.S. Code and state statutes are applicable and may be incorporated through Article 134. Under Title 18, a "minor" is any person under the age of 18.

(3) Some Federal statutes that pertain to Internet solicitation fall under Chapter 117, Title 18 U.S.C. (Transportation for Illegal Sexual Activity and Related Crimes). Internet solicitation investigations will be worked under case category 8B, Sex Abuse–Child.

Sections of Title 18 U.S.C. Chapter 117 applicable to sexual offenses	
Section	Title
2421	Transportation generally
2422	Coercion and enticement
2423	Transportation of minors/transportation with intent to engage in criminal sexual activity
2424	Filing factual statement about alien individual
2425	Use of interstate facilities to transmit information about a minor
2426	Repeat offender
2427	Inclusion of offenses relating to child pornography in definition of sexual activity for which any person can be charged with a criminal offense

c. An appropriate state penal code may apply, depending on the jurisdiction and/or victim(s) of this crime category.

34-6. Subcategory Definitions. The definitions in the following six subcategories of NCIS sexual offense investigations assume offenses committed after the June 28, 2012, UCMJ revision detailed in paragraph 34-5 (Criminal Law and Jurisdiction).

a. Sex Abuse–Child (8B). Used for violations of UCMJ Article 120b (rape, sexual assault, and sexual abuse of a child), as well as for other offenses against a person younger than 16 years of age that do not fit specific requirements of Child Exploitation (8E) investigations.

b. Child Exploitation (8E). Used for all investigations involving child pornography, online enticement of children, commercial sexual exploitation of children, and child sex tourism as defined in Appendix C.

c. Stalking (8K). Used for violations of UCMJ Article 120a, investigations involving any person who wrongfully engages in a course of conduct directed at a specific person that would cause a reasonable person to fear death or bodily harm, including sexual assault, to themselves or an immediate family member. By definition under Article 120a, "course of conduct" means a repeated maintenance of visual or physical proximity to a specific person or a repeated conveyance of verbal threat, written threats, or threats implied by conduct, or a combination of such threats directed toward a specific person. In addition to the objective element (reasonable person test), violation of Article 120a also requires that the conduct actually induced fear and that the offender knew or should have known that the victim would be placed in fear. An investigation may initially be opened under case category 7C (Communication of a Threat); however, if a pattern or repetitiveness arises, the case category must be changed to reflect an 8K.

d. Other Sexual Misconduct–Adult (8M). Used for violations of Article 120c (other sexual misconduct: indecent viewing, visual recording, broadcasting, forcible pandering, or indecent exposure), Article 125 (animals only), Article 134 (indecent language), and Article 134 (pandering and prostitution). Investigations include those involving adults engaged in adultery, indecent language, indecent exposure, pandering, prostitution, indecent viewing, visual recording, broadcasting, voyeurism, and bestiality.

e. Sexual Assault–Adult (8S). Used for violations of Article 120 (rape and sexual assault), Article 125 (forcible sodomy) and Title 18 U.S.C. Chapter 109A Sexual Abuse (sections 2241, 2242, and 2244). Investigations include those involving a rape, sexual assault, aggravated sexual contact, abusive sexual contact, and forcible sodomy of a person who has attained the age of 16.

f. Special Inquiry (8X). Investigations in this subcategory involve offenses that are not specifically covered by any other subcategories. Such inquiries normally require those investigative techniques utilized in cases within the basic category of sex offense investigations and will include interrogation where considered appropriate. If the victim is under 16 years of age, the investigation will be pursued under category 8B. When opening an 8X, the correct case category is "Special Inquiry," regardless of the offense.

34-7. Procedures. See Appendix D for investigative procedures for cases involving adult victims, and Appendix E for special considerations in cases involving child victims.

APPENDIX A
REFERENCES

(a) DoD Instruction 5505.18, Investigation of Adult Sexual Assault in the Department of Defense, 25 January 2013

(b) DoD Instruction 6495.02, Sexual Assault Prevention and Response (SAPR) Program Procedures, 28 March 2013 (Incorporating Change 1, Effective February 12, 2014)

(c) SECNAV Instruction 1752.4B, Sexual Assault Prevention and Response, 8 August 2013

(d) DoDIG Directive-Type Memorandum 14-002, The Establishment of Special Victim Capability (SVCV) Within the Military Criminal Investigative Organizations, 11 February 2014

(e) SECNAV Instruction 1752.3B, Family Advocacy Program (FAP), 10 November 2005

(f) DoD Directive 6400.1, Family Advocacy Program (FAP), 23 August 2004

(g) DoD Instruction 6400.06, Domestic Abuse Involving DoD Military and Certain Affiliated Personnel, 21 August 2007 (Incorporating Change 1, September 20, 2011)

(h) DoD Instruction 5505.14, Deoxyribonucleic Acid (DNA) Collection Requirements for Criminal Investigations, 27 May 2010

(i) DoD Instruction 1030.2, Victim and Witness Assistance Procedures, 4 June 2004

(j) DoD Directive 1030.01, Victim and Witness Assistance," 13 April 2004 (certified current as of April 23, 2007)

(k) NCIS-1, Chapter 25, Section 1, SSD Report Writing, January 2010

(l) 42 U.S.C. 10607, Crime Control Act of 1990

(m) 18 U.S.C. 3771, Crime Victim Rights Act of 2004

(n) 18 U.S.C. 3509, Child Victims' and Child Witnesses' Rights

(o) 18 U.S.C. 5038, Use of Juvenile Records

(p) 18 U.S.C. 4042, Duties of Bureau of Prisons

(q) SECNAV Instruction 5800.14A, Notice of Release of Military Offenders Convicted of Sex Offenses or Crimes Against Minors, 24 May 2005

(r) Adam Walsh Child Protection and Safety Act of 2006

APPENDIX B
ACRONYMS AND ABBREVIATIONS

AASVTP	Advanced Adult Sexual Violence Training Program
AFCCP	Armed Forces Center for Child Protection
AFSVTP	Advanced Family and Sexual Violence Training Program
ASAP	Adult Sexual Assault Program
AUSA	assistant United States attorney
CAR	case activity record
CASS	Command Authorized Search and Seizure
CCN	case control number
CEOS	Child Exploitation and Obscenity Section
CLEOC	Consolidated Law Enforcement Operations Center
CPII	Child Pornography Image Index
CPS	child protective services
CRIS	Child Recognition and Identification System
CVIP	Child Victim Identification Program
DAVA	domestic abuse victim advocate
DCFL	Defense Computer Forensic Laboratory
DCII	Defense Central Index of Investigations
DSAID	Defense Sexual Assault Incident Database
D-DEx	Law Enforcement Defense Data Exchange
DFSA	drug-facilitated sexual assault
EEE	Emergency and Extraordinary Expense
ESP	electronic service provider
FAP	Family Advocacy Program
FAR	Family Advocacy Representative
FBI	Federal Bureau of Investigation
FDE	Forensic Data Extraction
FIR	Field Information Report
IA	Investigative Action
ICAC	Internet Crimes Against Children
IP	Internet Protocol
ICE	Immigration and Customs Enforcement
ISP	Internet Service Provider
JPAS	Joint Personnel Adjudication System
K-Net	Knowledge Network
MCIO	military criminal investigative organization
MPO	Military Protective Order
MTF	military treatment facilities
NCIC	National Crime Information Center
NLETS	National Law Enforcement Telecommunication System
PASS	Permissive Authorization for Search and Seizure
ROI	report of investigation
RRCN	restricted reporting case number
SACMG	sexual assault case management group

APPENDIX B (CONT'D)
ACRONYMS AND ABBREVIATIONS

SAFE	sexual assault forensic exam
SANE	sexual assault nurse examiner
SAPR	sexual assault prevention and response
SARC	sexual assault response coordinator
SART	sexual assault response team
SJA	staff judge advocate
SMART	Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking
SMR	Sexual Maturity Rating
SORNA	Sexual Offender Registration and Notification Act
SSA	supervisory special agent
SVC	special victims capability
TCTP	Trial Component Training Program
UCMJ	Uniform Code of Military Justice
VIS	Victim Impact Statement
VLC	Victims Legal Counsel
VPS	Victim Preference Statement
VWAP	Victim and Witness Assistance Program

APPENDIX C
DEFINITIONS AND PREFERRED TERMS

It is preferred that appropriate anatomical or action terms be used in ROI documentation, vice the slang or street terms that a victim or subject may use during an interview. It is allowable and appropriate to use slang or street terms when taking a statement from someone, as a sworn statement should be in the interviewee's own words. Legal terms and phrases are copied from the UCMJ and need not be used in the investigation; accurate, factual descriptions are preferred to facilitate legal determinations. Below is a list of terms often encountered in sexual assault investigations.

abrasion: area of the body surface denuded of skin and mucous membrane by some unusual or abnormal mechanical process.

anus: anal orifice, which is the lower opening of the digestive track, lying in the fold between the buttocks.

bestiality (Article 125): carnal copulation with an animal; or taking the sexual organ of an animal into a person's mouth, vagina, or anus; or placing a person's sexual organ in the mouth, vagina, or anus of an animal.

broadcast (Article 120c): to electronically transmit a visual image with the intent that it be viewed by a person or persons.

cervix: portion of the uterus between the isthmus and the vagina.

child pornography (Article 134): material that contains either (a) an obscene visual depiction of a minor engaging in sexually explicit conduct or (b) a visual depiction of an actual minor engaging in sexually explicit conduct.

child sex tourism: traveling abroad for the purpose of sexually abusing children. Child sex tourists capitalize on their relative wealth and the lack of effective law enforcement in the destination countries to engage in illicit sex acts with children.

clitoris: small cylindrical erectile body situated at the anterior (superior) portion of the vulva (covered by a sheath of skin called the clitoral hood).

commercial sexual exploitation of children: recruitment and coercion of children into prostitution.

consent (Article 120): (a) Freely given agreement to the conduct at issue by a competent person. An expression of lack of consent through words or conduct means there is no consent. Lack of verbal or physical resistance or submission resulting from the use of force, threat of force, or placing another person in fear does not constitute consent. A current or previous dating or social relationship by itself or the manner of dress of the person involved with the accused in the conduct at issue shall not constitute consent. (b) A sleeping, unconscious, or incompetent

APPENDIX C (CONT'D)
DEFINITIONS AND PREFERRED TERMS

person cannot consent. A person cannot consent to force causing or likely to cause death or grievous bodily harm or to being rendered unconscious. A person cannot consent while under threat or fear or in response to a fraudulent representation that the sexual act serves a professional purpose or having been induced by artifice, pretense, or concealment that the person is another. (c) Lack of consent may be inferred based on circumstances of the offense. All the surrounding circumstances are to be considered in determining whether a person gave consent, or whether a person did not resist or ceased to resist only because of another person's actions.

consent (Article 120b): lack of consent is not an element and need not be proven in any prosecution under Article 120b. A child not legally married to the person committing the sexual act, lewd act, or use of force cannot consent to any sexual act, lewd act, or use of force.

contusion: bruise; superficial injury produced from impact without laceration.

course of conduct (Article 120a): (a) a repeated maintenance of visual or physical proximity to a specific person; or (b) a repeated conveyance of verbal threat, written threats, or threats implied by conduct, or a combination of such threats, directed at or toward a specific person.

cunnilingus: oral stimulation of the vulva or clitoris.

erection: when the penis fills with blood and is rigid; occurs when the male is in a sexually excited state.

fellatio: oral stimulation of the penis.

force: (a) use of a weapon; (b) the use of such physical strength or violence as is sufficient to overcome, restrain, or injure a person; or (c) inflicting physical harm sufficient to coerce or compel submission by the victim. For a child, it is also sufficient merely to inflict physical harm or, in the case of a parent-child or similar relationship, the use or abuse of parental or similar authority is sufficient to constitute the use of force.

hymen orifice: opening to the vagina through the hymenal membrane.

hymen: membrane that partially, or rarely completely, covers the external vaginal orifice. It is located at the junction to the vestibular floor and the vaginal canal.

indecent broadcasting (Article 120c): knowingly broadcasting or distributing any recording that the person knew or reasonably should have known was made under circumstances described by indecent viewing and indecent visual recording.

indecent viewing (Article 120c): knowingly and wrongfully viewing the private area of another person, without that other person's consent and under circumstances in which that other person has a reasonable expectation of privacy.

APPENDIX C (CONT'D)
DEFINITIONS AND PREFERRED TERMS

indecent visual recording (Article 120c): knowingly photographing, videotaping, filming, or recording by any means the private area of another person without that other person's consent and under circumstances in which that other person has a reasonable expectation of privacy.

labia majora: rounded folds of skin forming the lateral boundaries of the vulva.

labia minora: longitudinal, thin folds of tissue within the labia majora. In the prepubescent child, these folds extend from the clitoral hood to approximately the midpoint on the lateral wall of the vestibule. In the adult, they enclose the vestibule and contain the opening to the vagina.

laceration: wound made by tearing.

lewd act (Article 120b): (a) any sexual contact with a child; (b) intentionally exposing one's genitalia, anus, buttocks, or female areola or nipple to a child by any means, including via any communication technology, with intent to abuse, humiliate, or degrade any person, or to arouse or gratify the sexual desire of any person; (c) intentionally communicating indecent language to a child by any means, including via any communication technology, with an intent to abuse, humiliate, or degrade any person, or to arouse or gratify the sexual desire of any person; or (4) any indecent conduct, intentionally done with or in the presence of a child, including via any communication technology, that amounts to a form of immorality relating to sexual impurity which is grossly vulgar, obscene, and repugnant to common propriety, and tends to excite sexual desire or deprave morals with respect to sexual relations.

online enticement of children: the use of the Internet to entice and manipulate children into situations in which they become vulnerable to sexual exploitation, particularly child pornography, sexual contact, and abduction. Related investigations include "travelers," in which online predators travel to the location of a child for the purpose of establishing physical contact.

oral copulation: mouth-to-genital contact or genital-to-mouth contact.

paraphilia: recurrent, intense and sexually arousing fantasies, urges, or behavior that generally involve nonhuman objects, the suffering or humiliation of oneself or one's partner, or children or other nonconsenting persons and that occur over a period of at least 6 months. Some examples of paraphilias include exhibitionism, fetishism, frotteurism, pedophilia, sexual masochism, sexual sadism, and voyeurism.

penis: male sex organ composed of erectile tissue through which the urethra passes.

posterior fourchette: junction of the two labia minora posteriorly (inferiorly). This area is referred to as a posterior commissure in the prepubescent child. In children, the labia minora are not completely developed and do not connect inferiorly until puberty. In the postpubescent female, it is referred to as the posterior fourchette.

APPENDIX C (CONT'D)
DEFINITIONS AND PREFERRED TERMS

private area (Article 120c): naked or underwear-clad genitalia, anus, buttocks, or female areola or nipple.

prostitution (Article 120c): a sexual act or sexual contact on account of which anything of value is given to, or received by, any person. Note: the definition under Article 134 is limited to adulterous (vaginal) sexual intercourse.

rectum: distal portion of the large intestine that ends at the anal canal.

scrotum: pouch that contains the testicles and their accessory glands.

sexual act: (a) contact between the penis and the vulva or anus or mouth, upon penetration, however slight; or (b) the penetration, however slight, of the vulva or anus or mouth of another by any part of the body or by any object, with an intent to abuse, humiliate, harass, or degrade any person or to arouse or gratify the sexual desire of any person.

sexual contact: (a) touching, or causing another person to touch, either directly or through the clothing, the genitalia, anus, groin, breast, inner thigh, or buttocks of any person, with an intent to abuse, humiliate, or degrade any person; or (b) any touching, or causing another person to touch, either directly or through the clothing, any body part of any person, if done with an intent to arouse or gratify the sexual desire of any person.

sexually explicit conduct (Title 18): actual or simulated sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic area of any person.

stalking (Article 120a): wrongfully engaging in a course of conduct which would cause a reasonable person to fear death or bodily harm, including sexual assault, to himself or herself or a member of his or her immediate family, with knowledge that acts will place a specific person in reasonable fear, and where the acts do induce a reasonable fear.

threatening or placing child in fear: a communication or action that is of sufficient consequence to cause the child to fear that non-compliance will result in the child or another person being subjected to the action contemplated by the communication or action.

vagina: uterovaginal (genital) canal in the female. This internal structure extends from the uterine cervix to the inner aspect of the hymen.

vulva: external genitalia or pudendum of the female. It includes the mons pubis (fatty area over the pubic bone), clitoris, labia majora, labia minora, vaginal vestibule (cavity containing the opening to the vagina and the urethra), urethral orifice, vaginal orifice, hymen, and the posterior fourchette.

Pages 1024 through 1052 redacted for the following reasons:
- -
(b)(7)(E)

APPENDIX F
FAMILY ADVOCACY PROGRAM

1. The mission of the Family Advocacy Program, or FAP, under reference (e) is to promote public awareness within the military and civilian communities and coordinate professional intervention at all levels, including law enforcement, social services, health organizations, and legal entities. FAP is designed to break the cycle of abuse by identifying abuse as early as possible and by providing treatment to the affected family member. FAP works with individuals and families to strengthen family relationships and prevent child and spouse maltreatment. The program is dedicated to enhancing individual coping skills and alleviating the underlying causes of stress associated with family violence. FAP also provides education services in child abuse, spouse and family violence, parenting, and stress management. The objectives of FAP are to prevent spouse and child abuse, to encourage the reporting of all instances of such abuse, to ensure the prompt assessment and investigation of all abuse cases, to protect victims of abuse, and to treat all family members affected by or involved in abuse.

2. Interaction with criminal investigations. FAP is a support system for members who are suitable for rehabilitation and retention based on a command determination using an appropriate medical/counselor recommendation. FAP is not a substitute for disciplinary action. FAP does not prohibit or hinder the completion of an investigation by NCIS into allegations of criminal conduct. If NCIS opens an investigation based on information gained through FAP, FAP staff shall coordinate with NCIS prior to interviewing or otherwise assessing suspected offenders.

3. Notification to NCIS. FAP has guidelines concerning NCIS notifications. FAP will notify NCIS in all cases of child sex abuse, serious domestic abuse (unless under restricted reporting), family-related incidents involving stalking or other threatening behavior, threatening with or use of a weapon, strangulation, and any abuse that results in a fatality or injury. FAP will notify NCIS if allegations of child pornography are developed during the course of a FAP case. The FAP will annotate consultation with NCIS in the victim's FAP record book. Cases not opened by NCIS should be referred to base security/police.

4. Allegations arising during emergency treatment. When an allegation or suspicion of criminal conduct is raised during emergency medical treatment, the attending medical or command personnel must seek appropriate investigative assistance from NCIS except in instances of restricted reporting). Liaison with local civilian law enforcement agencies is the responsibility of NCIS.

5. Confidentiality. Information received about FAP clients must be treated with the highest degree of confidentiality and protected within the rules and intent of the Privacy Act.

APPENDIX G
SEX OFFENDER REGISTRATION

1. Various state and federal laws require the registration of sex offenders with state law enforcement agencies. Each state determines the criteria for registration and notification, which is the means by which law enforcement disperses information to the public. Additional information regarding sex offender registration can be found at the U.S. Department of Justice National Sex Offender Public Website.[13] In addition, the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking[14] (SMART) aims to protect the public by supporting national implementation and provides guidance and technical assistance.

2. Duties of prisons and confinement facilities. Pursuant to reference (p), the Federal Bureau of Prisons, upon release of a designated sex offender from prison or upon an offender's sentence to probation, must provide notice to the chief law enforcement officer of the state and local jurisdiction in which the offender will reside and to the state or local agency responsible for the receipt and maintenance of sex offender registration information in the state or local jurisdiction in which the offender will reside. Military confinement facilities have similar responsibilities, see reference (q). Because offenders do not always self-register as required, the DoD manages a notification program for military offenders who have been adjudged guilty of qualifying sex offenses or crimes against minors at special or general courts-martial. Military confinement facilities are responsible for ensuring notice to the proper authorities prior to the permanent release of a prisoner for whom sex offender notification is required.

3. The Sexual Offender Registration and Notification Act (SORNA). In accordance with reference (r), the SORNA reformed some of the older sexual offender registration laws. It extends the jurisdictions in which registration is required beyond the 50 States, the District of Columbia, and the principal U.S. territories, to include Indian tribal jurisdictions, and extends the classes of sex offenders and sex offenses for which registration is required. The SORNA requires that sex offenders in the covered classes register and keep the registration current in the jurisdictions in which they reside, work, or go to school. Covered offenses include most sexual acts and contact, attempts, and child sex offenses.

4. Overseas applicability. The SORNA contains language pertaining to registered sex offenders who live overseas. A sex offender who goes abroad may remain subject in some respects to U.S. jurisdiction. For example, a sex offender may leave to live on an overseas U.S. military base as a Service member, dependent, or employee or to work for a U.S. military contractor in another country. In such cases, notification about the individual's status as a sex offender and intended activities abroad is of interest to Federal authorities. The following requirements apply to sex offenders who leave the United States. Each jurisdiction in which a sex offender is registered as a resident requires the sex offender to inform the jurisdiction if the sex offender intends to commence residence, employment, or school attendance outside of the United States. Once the information is received, the jurisdiction must: (1) notify all other jurisdictions in which the sex offender is required to register through immediate electronic forwarding of the sex offender's

[13] http://www.nsopw.gov
[14] http://www.smart.gov

registration information (including the sex offender's expected residence, employment, or school attendance outside of the United States) and (2) notify the U.S. Marshals Service and update the sex offender's registration information in the national databases.

5. NCIS field office responsibility. NCIS must make notification when confinement facilities are not involved. Reference (p) lists qualifying offenses, without referring to recent UCMJ updates; however, the SORNA requires that the military offenses identified by the Secretary of Defense as registration offenses be at least as broad as the SORNA definition.

a. Convening Authority action. The convening authority, or the convening authority's designee, must notify NCIS no later than one day after completion of judicial proceedings at a special or general courts-martial that results in conviction of a qualifying sex offense or crime against a minor when those offenders meet one of the following criteria: (1) not sentenced to any confinement (or all confinement is suspended), (2) not confined in a Service-operated confinement facility, or (3) not under control of the U.S. Probation Office or Federal Bureau of Prisons at the time of release from military service. The Convening Authority will provide NCIS with the Reports of Results of Trial, indicating any sex offender registration or notification requirement to be accomplished, and documentation of the offender's intended address of residence. Notification must also be given to NCIS immediately upon completion of any post-trial action that would affect the Service member's reporting requirements.

b. NCIS notifications. Upon receiving notice from the Convening Authority of those military offenders meeting the criteria of a qualifying sex offense, the NCIS field office must ensure notifications are made using DD Form 2791 within 10 days of completion of judicial proceedings. If the offender is being released to a location within the United States, the following officials must be notified using DD Form 2791: (1) the chief law enforcement officer of the State in which the prisoner intends to reside, (2) the chief law enforcement officer of the local jurisdiction in which the prisoner intends to reside, and (3) the State or local agency responsible for the receipt or maintenance of a sex offender registration in the State or local jurisdiction in which the prisoner intends to reside. The case agent, prior to the closure of a sex investigation that meets the criteria of a qualifying sex offense, must include DD Form 2791 as an exhibit to the ROI (CLOSED). Upon closure of a case, the SSA must certify the case agent accomplished the sex offender registry notification, as noted on the Closed Case Certification/Release sheet.

c. Overseas. If the offender is planning to live outside the United States, written notice of the offender's return using DD Form 2791 must be made in accordance with the laws of the country of destination.

d. Change in conviction status. In the event of post-trial action disapproving all findings, (no conviction for a sex offense or crime against a minor is approved), NCIS must ensure prompt notice via memorandum to all recipients of notifications that the previous notice is withdrawn. Cases that are appealed should be held in extended retention until all action is complete.

APPENDIX G (CONT'D)
SEX OFFENDER REGISTRATION

6. DON facilities. Reference (q) restricts access of convicted sex offenders to Navy facilities: "To the maximum extent permitted by law, unless waived by competent authority, sex offenders are to be identified and prohibited from accessing Navy facilities." This policy applies to active-duty personnel, their family members, and DoD civilian and contractor employees.

CHAPTER 35
TITLE: PROTECTIVE OPERATIONS
POC: CODE 21B
DATE: SEP 07

35-1. PROTECTIVE OPERATIONS OVERVIEW.

a. The purpose of this chapter is to acquaint all Naval Criminal Investigative Service (NCIS) personnel with the basic elements of protection and the types of protective operations that NCIS provides, and to provide relevant guidance on policy, reporting, and the overall

conduct of protective operations. The term “protective operations” is generally defined to be all security and law enforcement measures taken to identify threats or vulnerabilities to specific principals and/or to provide security for those principals.

b. Protective operations are an integral part of the NCIS mission and a vital service to the Department of the Navy (DON), the Department of Defense (DOD), and the United States Government. NCIS Protective Operations Program involves a wide range of support to DON, DOD, and non-DOD agencies. NCIS protective operations are managed under the NCIS Combating Terrorism Directorate by the Protective Operations Department (Code 21B). Protective Operations are considered a priority operational requirement for NCIS.

c. All protective operations support is conducted at the direction and under the authorization of the Deputy Assistant Director (DAD) for Protective Operations, acting on behalf of the Director, NCIS. Protective operations must be authorized and coordinated in advance by Code 21B, unless an exigent or emergency situation exists. Under emergency circumstances, telephonic notification of Code 21B will suffice. Protective operations may be undertaken for the following reasons:

(1) When recommended by a Personal Security Vulnerability Assessment (PSVA).

(2) Due to an increase in the general threat within an area or region.

(3) In response to a specific threat to an individual.

(4) Following a request for support from DOD, DON or another U.S. Government agency.

(5) In response to special circumstances or events (when approved by NCISHQ).

d. Throughout this chapter, the term “NCIS personnel” is used to identify those individuals who support protective operations. This includes, but is not limited to: civilian Special Agents (GS-1811), NCIS Marine Corps Special Agents, Navy Reserve Officers in the NCIS unit (credentialed as NCIS Agents), civilian Investigators (GS-1810), Security Specialists (GS-0080), Masters-at-Arms (credentialed as NCIS Investigators), and United States Navy/United States Marine Corps (USN/USMC) security personnel supplementing protective operations.

e. For additional terms, see Appendix 1 (Glossary of Terms) and Appendix 2 (Radio Communications Glossary).

35-2. AUTHORITY.

a. Authority for NCIS to conduct protective operations is based upon the following laws, as well as DOD, SECNAV, and DON directives and instructions. Links to the Internet sites for the U.S. Code (USC), DOD, and DON directives and instructions are located in Appendix 3 (References) to this chapter.

b. DOD Directive 2000.12 creates the broad antiterrorism (AT) policy and authorizes the DOD AT standards (DOD Instruction 2000.16) and the DOD Antiterrorism Handbook (DOD O-2000.12-H). DOD Directive 2000.12 also identifies the appropriate DOD official who has cognizance for protective operations and instructs the Secretaries of the Military Departments to identify the high-risk billets in their Departments and provide appropriate AT training.

c. DOD Instruction 2000.16 identifies the AT standards required. Of particular interest to protective operations is DOD Standard 25 “Training for High-Risk Personnel and High-Risk Billets” and DOD Standard 31 “Executive Protection and High Risk Personnel Security.”

d. The DOD Antiterrorism Handbook (O-2000.12-H) recognizes, in Chapter 21, Section C21.10:

PROTECTIVE SECURITY OPERATIONS
C21.10.1. Each Department is authorized to provide Protective Security Details (PSD) for key senior military officers, DOD civilians, other U.S. Government officials or foreign dignitaries requiring personal protection.

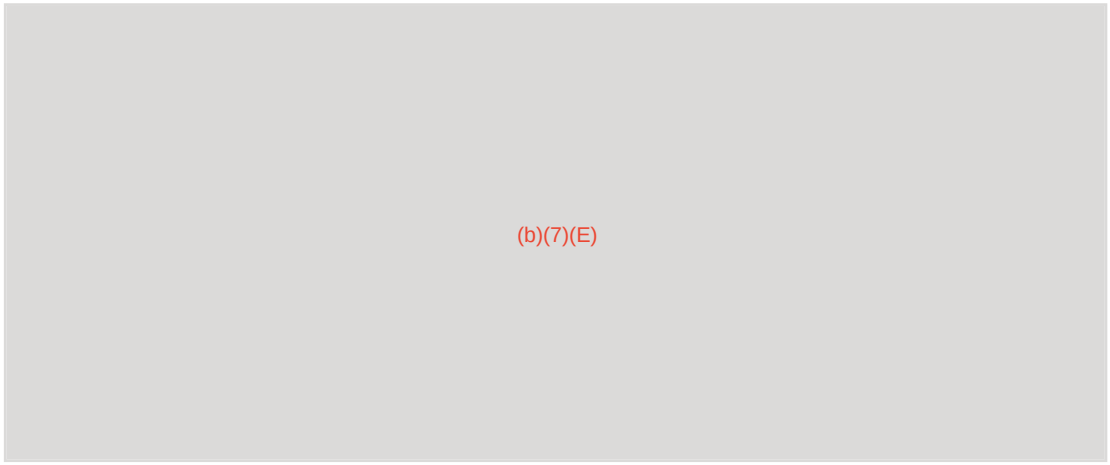
C21.10.2. Each Department’s Secretary upon recommendations of their counterintelligence and/or law enforcement investigation staffs makes assignment of PSDs to executives. PSDs are assigned to DOD personnel who meet requirements established by Service regulations. In general, PSDs may be assigned only to those executives whose position or assignment places them at risk and whose continued availability to the President, Secretary of Defense, and Combatant Commanders is vital to the execution of DOD missions.

e. 10 U.S. Code 1585, implemented by DOD Directive 5210.56 and SECNAVINST 5500.29C "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," authorizes the arming of NCIS law enforcement personnel and the carrying of weapons while providing protective operations support to DOD officials and foreign dignitaries.

f. Within the NCIS charter document, SECNAVINST 5430.107 “Missions and Functions of the Naval Criminal Investigative Service,” NCIS is designated as the primary investigative and counterintelligence agency for DON. The SECNAVINST further identifies NCIS as the executive agent for all Protective Service matters within DON. NCIS shall execute exclusive jurisdiction and authority to conduct and coordinate Protective Service Operations to protect individuals who occupy designated DON High Risk Billets (HRBs), and other designated individuals, except as otherwise authorized by a combatant commander in a Joint Operating Area.

g. OPNAVINST 3300.55 and OPNAVINST 3300.53 further assign responsibility to Director, NCIS to maintain the DON HRB list and briefing program, provide protective services, and to provide DON armored vehicle support. Further, enclosure (11) to OPNAVINST 3300.53 states that only NCIS will perform protective operations, with specific restrictions on local commands’ authorities and abilities.

35-3. PROTECTION REQUEST AND APPROVAL PROCEDURES.



b. The degree of threat and vulnerability of designated billets and/or personnel will determine the level and/or type of protective operations support provided. Protocol, rank, seniority, and/or official positions are NOT viewed as reasons to justify protective operations.

c. All protective operations support will be approved in advance by the DAD, Code 21B (acting on behalf of the Director, NCIS), or his designee, unless there is an exigent or emergency circumstance. In the event of an exigent or emergency situation, protective operations support may be initiated by any trained NCIS Special Agent and Code 21B will be notified by the most expeditious means possible for guidance, assistance and support.

d. In an effort to standardize protective operations requests that arise from local commands, the following policy has been adopted. Commands that believe that there is a need for protective operations support in their AOR will draft a letter to the local NCIS office documenting the need for protection. This letter should be on command letterhead and will include the following information (at a minimum):

(1) Name and rank of potential principal;

(2) Title of principal's billet;

(3) Country of affiliation;

(4) Anticipated itinerary;

(5) Portion of itinerary that requires protection (if not entire mission);

(6) Reasons for request for protection; and

(7) Supporting information (threats, etc.).

e. Upon receipt of the written request, the local NCIS office supervisor will prepare a brief message either supporting or opposing the command's request. Both the command request and local NCIS office message will then be forwarded to the Protective Operations Department

(Attention: Operations Supervisor). Code 21B will review the request and provide guidance to the field as to the appropriate level of support, if any, to be provided.

f. Local commands may not initiate their own protective service details or other armed security escorts without consulting with the local NCIS office. Local commands are prohibited, under SECNAVINST, and OPNAVINST 5500.33c, from conducting protective operations off base unless working under the control of NCIS.

35-4. FIELD OFFICE TASKING AND STAFFING OF PROTECTIVE OPERATIONS.

a. Support from NCIS field offices and their subordinate offices is critical to the success of protective operations, whether the tasking is to support a DON principal, a DOD principal, or other U.S. or foreign dignitaries.

b. In order to facilitate tasking of missions, it is highly recommended that each field office designate one (1) Special Agent, Investigator, or supervisor to serve as the Field Office Protective Operations point of contact. Code 21B will task support requirements to this individual for action at the field office level. This will include support to DOD principals and DOD foreign visitors. Additionally, NCIS PSAs will task requirements directly to this individual when DON principals and DON foreign visitors come to field office AOR.

c. Code 21B and the Multiple Threat Alert Center (MTAC) will be notified in advance of all protective operation travels. In missions tasked by NCISHQ, Code 21B will facilitate country clearance and weapons authorization issues. In instances where NCIS Special Agents are supporting Army CID Protective Service Unit (PSU) missions, Army CID PSU will assume these notification responsibilities.

35-5. HIGH-RISK BILLET (HRB).

a. Under SECNAVINST 5430.107, Code 21B participates with OPNAV N3AT and HQMC in the process to identify, review and validate DON HRBs. In early January of each year, N3AT queries DON Echelon II Commanders for nominations of billets under their command that are potentially at high-risk to terrorist activities. These billets are identified based upon the grade, assignment, geographic location, travel itinerary and/or symbolic value that may make them attractive and/or accessible terrorist targets. Commanders are requested to list their nominees under one of two categories; (1) a level I HRB, requiring NCIS to conduct a Personal Security Vulnerability Assessment (PSVA) on that person or; (2) a level II HRB, enabling the nominee to receive en route anti-terrorism training sponsored by the DON.

b. Nominations are received by the end of January. In February of each year, a HRB Board is convened to review the list of nominations, determine HRB eligibility/ necessity, and subsequently validate HRB status as Level I or Level II. This HRB Board is comprised of representatives from OPNAV N3AT, HQMC and NCIS Code 21B, and is chaired by the DAD, NCIS Protective Operations Department. Following completion of the board, a list of validated HRBs for the calendar year is published to the Navy and Marine Corps Echelon II commands via naval message.

c. Billets validated as a Level I HRB will be scheduled during that calendar year for a NCIS PSVA. Those billets validated as a Level II HRB will be identified to the Commander, Navy Personnel Command for appropriate training. Although nominations are solicited in January, this does not preclude new nominations from being submitted when the situation changes significantly regarding terrorist activities, or when there is a specific need.

d. Generally, NCIS protective operations support is provided only to individuals who occupy positions designated as Department of the Navy HRBs. Certain other DON officials may also be provided NCIS protective operations support on a case-by-case basis. Protective operations are predicated on an assessment that some level of threat to an individual or billet exists. This threat may be either explicit or implicit, such as in cases where a principal holds a position of a symbolic or public nature.

35-6. PERSONAL SECURITY VULNERABILITY ASSESSMENT (PSVA).

a. Code 21B manages the PSVA process under SECNAVINST 5430.107. After the list of validated HRBs is published each year, personnel from Code 21B will schedule PSVAs to be conducted throughout the calendar year. Assessments are conducted via a Vulnerability Assessment (5V investigation) and are controlled and tasked solely by Code 21B. The assessment is normally conducted by Code 21B personnel or in concert with outlying local NCIS offices and/or personnel from the Security Training Assistance Assessment Team (STAAT). Once completed, the assessment and recommendations conducted by the field will be forwarded to Code 21B for evaluation and review. Code 21B is the final authority regarding recommendations contained in the PSVA, and will publish the final report documenting any recommendations. A PSVA is valid for 3 years unless there are changes to the threat environment, HRB residence and/or work location, or the HRB incumbent transfers and is replaced. Code 21B will continue to monitor these factors during that timeframe, and will generate documentation to that effect each year, which will remain in the HRB PSVA file for that position.

b. The purpose of the NCIS PSVA is to assess the following: (1) an HRB's level of risk and vulnerability to criminal or terrorist activities; (2) identify current weaknesses in security plans, programs, or personal protection; and (3) make recommendations to correct identified weaknesses and/or enhance the HRB's overall security posture. The PSVA also may list recommended protective operations support if deemed necessary. Protective operations support can come in the form of a Personal Security Advisor (PSA), Personal Security Detail (PSD) or a combination thereof. The PSVA process is applied to all DON HRBs. Occasionally, based on special circumstances approved by Code 21B, a PSVA will be conducted on an individual or billet not designated as a HRB.

c. The PSVA examines the following ten areas: specific and identified terrorism threats, command terrorist threat reporting and information flow, overall general criminal threat, the HRB's position, the HRB's personal and command security awareness, (b)(7)(E) (b)(7)(E) In order to assist in compiling the information needed for the PSVA, a questionnaire addressing these areas has been developed to provide guidance.

d. Upon review by Code 21B, the completed PSVA along with a cover letter from the DAD for Code 21B will be forwarded, via a lead, to the effected office for dissemination to the HRB. It is recommended that a senior representative from the field office personally brief the HRB on the results of the PSVA, discuss security recommendations and the implementation of protective operations support, if recommended. In those instances in which a PSA and/or greater level of support is recommended, Code 21B personnel may be present for such briefings to facilitate detailed discussion. If the HRB incumbent does not agree with the recommendations of the PSVA, or declines the recommended level of support, the respective NCIS field office will document such and forward this information to Code 21B.

35-7. SUPPORT TO THE UNITED STATES SECRET SERVICE.

a. The protective responsibilities of the United States Secret Service (USSS) are outlined in Title 18 U.S. Code, Section 3056. DOD Instruction 5030.34 "Agreement Between the United States Secret Service and the Department of Defense Concerning Protection of the President and Other Officials" identifies the DOD response to assist the USSS. NCIS personnel providing such support are subject to the overall supervision of the Director, USSS. NCIS has primary jurisdiction within the DON for support to the USSS and other DOD and non-DOD agencies conducting Protective Service Operations for U.S. government and foreign officials.

b. Regardless of method received, USSS requests for assistance in protecting the President or Vice-President will be honored and complied with immediately. USSS requests for support to other USSS principals will be approved through Code 21B, unless exigent circumstances apply. Normally, USSS requests are made to Code 21B in advance, who will then notify the appropriate NCIS field element.

c. USSS will normally request NCIS protective operations support for visits to DON facilities or in geographic areas where NCIS has a presence and the USSS does not. USSS may also make requests for NCIS support as part of the USSS responsibility for any National Special Security Event (such as the Super Bowl or Inauguration ceremonies).

d. All protective operations support will be documented via a ROI utilizing category 9A and will include Code 21B on distribution.

35-8. SUPPORT TO MISSIONS FOR SENIOR DEPARTMENT OF DEFENSE PERSONNEL.

a. NCIS is mandated, by direction of the Secretary of Defense, to support the Army CID Protective Services Unit (PSU) in its mission as Executive Agent for the protection of the Secretary of Defense (SECDEF), Deputy Secretary of Defense (DEPSECDEF), Chairman of the Joint Chiefs of Staff (CJCS), and the Vice-Chairman of the Joint Chiefs of Staff (VCJS).

b. In these operations, Army CID is the lead agency and NCIS acts as a supporting element. Each month, the Army CID PSU will provide Code 21B with the anticipated monthly travel calendar and tasking information.

c. Upon receipt of tasking and review, Code 21B will initiate a category 9A ROI (OPEN), which will outline support required from NCIS, and forward lead tasking to the appropriate NCIS field office(s). The cognizant field EAD will also be copied on the tasking. Field elements are required to support the DOD protective tasking; however, coordination with Code 21B may be required in order to fulfill these tasking.

d. Army CID PSU funds travel costs, lodging and per diem for these missions. NCIS personnel detailed to Army CID PSU missions are subject to Army CID PSU rules and regulations and fall under the operational control of the Mission Special Agent in Charge (MSAC) from Army CID PSU.

e. All protective operations support will be documented via a ROI utilizing category 9A and will include Code 21B on distribution.

35-9. SUPPORT TO MISSIONS OF THE DEFENSE FOREIGN LIAISON OFFICE.

a. The Defense Foreign Liaison Office (DFLO), within the Office of Secretary of Defense, is responsible for planning, coordinating, and overseeing foreign counterpart visits for the Secretary of Defense (SECDEF), Deputy Secretary of Defense (DEPSECDEF), Chairman of the Joint Chiefs of Staff (CJCS), and the Vice-Chairman of the Joint Chiefs of Staff (VCJS). DFLO is responsible for coordinating all aspects of the visit, including transportation, lodging, meals and official visits.

b. A foreign Minister of Defense (MOD) is considered the equivalent of SECDEF/DEPSECDEF and a foreign Chairman of Defense (CHOD) is considered the equivalent of the CJCS/VCJCS. Titles will vary from country to country but will fall into one of these two categories. For protocol purposes during their visit, the counterpart assumes a rank higher than their host. For example, the visiting MOD of anywhere would, for the duration of his/her stay, be considered of higher rank than SECDEF, for protocol purposes only.

c. As part of this coordination, security arrangements are rotated between the military criminal investigative organizations (MCIOs): Army CID, Air Force OSI, and NCIS. NCIS is required, by direction from the Secretary of Defense, to support these visits. When the counterpart visit is scheduled, the next MCIO on the list is assigned to the visit. In some cases, foreign counterparts or their security teams may request a specific agency.

d. The MCIOs are required to provide at least the same level of support to the counterparts that the counterpart country would provide to the equivalent U.S. official. Remember that when the equivalent U.S. official travels overseas, the host will provide security assistance to U.S. security teams. Some counterpart visits will include their own security personnel (armed or unarmed), depending on State Department approval.

e. When NCIS is tasked to support these visits, Code 21B will receive the request, review the itinerary, determine the staffing requirements and forward lead tasking, via ROI (OPEN), to the affected field elements (as required).

f. If the counterpart is assigned a PSA from one MCIO and travels to an area that the MCIO does not cover (such as a NCIS PSA traveling to an Air Force or Army facility), coordination will be made by the PSA to the local MCIO office for any support issues.

g. All protective operations support will be documented via a ROI utilizing category 9A and will include Code 21B on distribution.

35-10. SUPPORT TO DEPARTMENT OF NAVY MISSIONS.

a. Within the DON, two elements are responsible for the coordination of foreign counterpart visits.

b. The Navy Foreign Liaison Office (NFLO) is the Executive Agent responsible for Chief of Naval Operations (CNO) counterpart missions. These missions are tasked directly from the NFLO office to the Protective Operations Department (CNO Protective Detail). A determination of threat and the level of security support to be provided, if any, will then be made by the PSA to the CNO. Support may include the full range of protective operations support.

c. The Marine Corps Special Projects Directorate (USMC SPD) is the Executive Agent responsible for Commandant of the Marine Corps (CMC) counterpart missions. These missions are tasked directly from the USMC SPD office to the Protective Operations Department (CMC Protective Detail). A determination of threat and the level of security support to be provided, if any, will then be made, by the PSA to the CMC. Support may include the full range of protective operations support.

d. All protective operations support will be documented via a ROI utilizing category 9A and will include Code 21B on distribution.

35-11. PERSONAL SECURITY ADVISOR.

a. Personal Security Advisor (PSA) is perhaps the most critical element of NCIS Protective Operations Program. After the completion of a PSVA that recommends PSA support, NCISHQ will select a NCIS Special Agent PSA. PSA responsibilities vary with the nature of each protective billet. The primary role of the PSA, as the name implies, is that of an advisor. A close, professional relationship must be developed between the principal, his/her staff, the local NCIS field office(s), and the PSA. The PSA is the NCIS conduit and focal point for the flow of NCIS information and support relative to the personal security of the principal. The operational functions of the PSA are as follows:

(1) Provide security advice to the principal, family and staff;

(2) Provide the “close-in” personal security for the principal as required;

(3) Provide liaison between the principal, NCIS, and U.S. and foreign law enforcement and intelligence agencies;

(4) Provide security support (using sound law enforcement principles) by

resolving minor incidents and supporting the cover and evacuation of the principal in major incidents;

(5) Designate responsibilities for personnel who are supporting the PSA's protective operations, whether full-time or temporarily; and

(6) Serve as the Detail Leader for whatever level of protective operations support is provided to the principal.

(b)(7)(E)

c. The PSA is responsible for providing thorough briefings to the principal as required. Principals who are unfamiliar with protective operations should be briefed regarding what NCIS personnel will do in emergency situations. PSAs must stress that protective personnel are providing a security function, and are not there for the convenience of the principal. Another important aspect is to ensure that the key personnel on the principal's staff understand the role of protective operations, as well as what to expect and what not to expect from the PSA and/or protective detail.

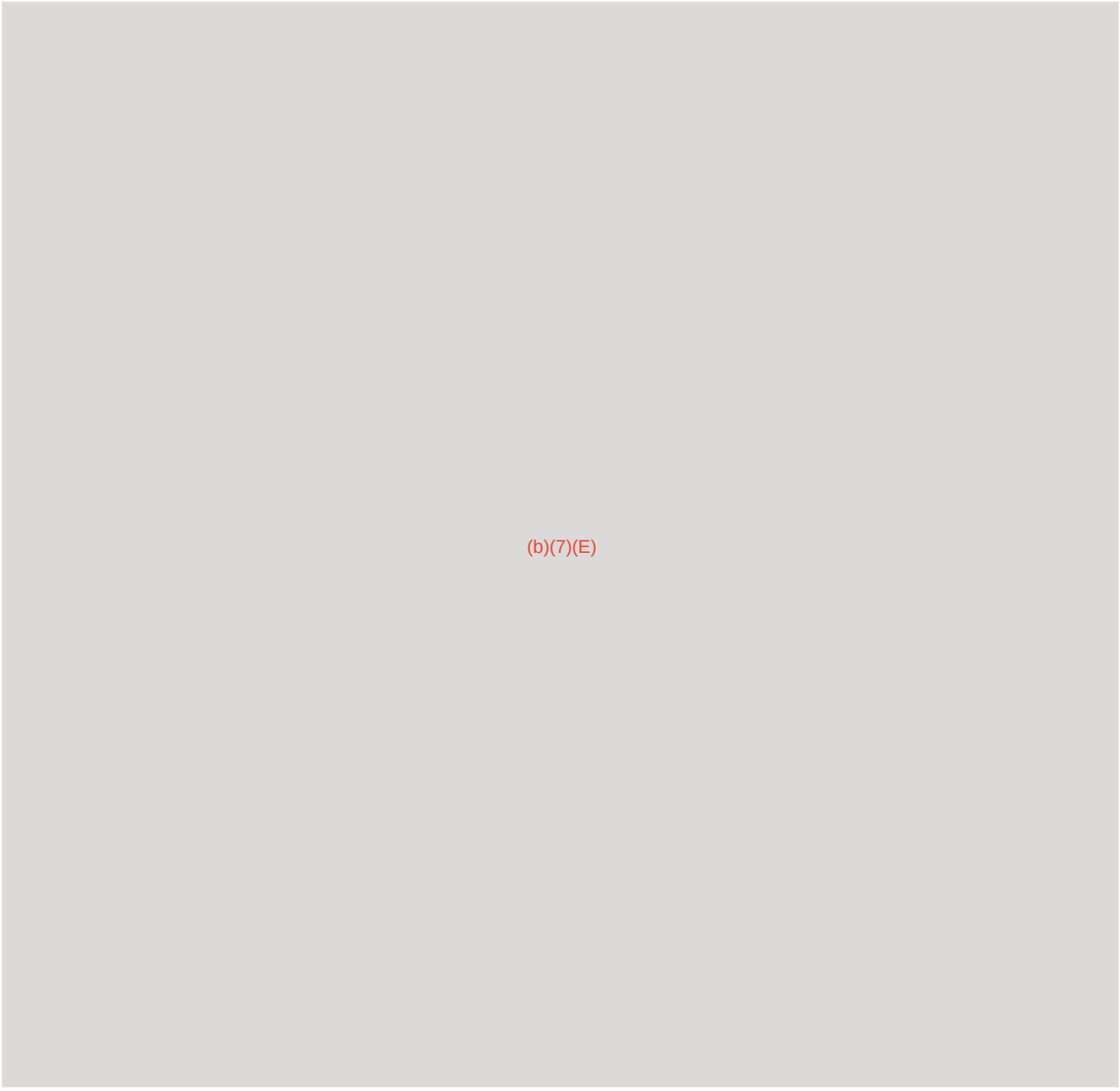
d. During an operation in support of a DON HRB to which a PSA is assigned on either a full or part-time basis, the PSA is expected to have a close, professional working relationship with the principal's staff and be able to coordinate all security aspects of an operation independently.

35-12. PROTECTIVE SERVICE DETAILS.

a. A Protective Service Detail (PSD) is the highest level of protective operations in the graduated response to increasing threat and vulnerability. A PSD is activated when there is credible information that the principal is a specific target. The nature of the threat may necessitate the initiation of a PSD simultaneously with the initiation of other protective measures. However, the initiation of a PSD is not dependent on any other variables, if the threat is initially deemed credible.

(b)(7)(E)

Pages 1067 through 1075 redacted for the following reasons:
- -
(b)(7)(E)



35-22. CLASSIFICATION OF ITINERARY.

a. DOD Directive 4500.54 directs that detailed foreign travel itineraries of DOD civilian officials appointed by the President, as well as all members of the Joint Chiefs' of Staff, shall be classified "CONFIDENTIAL," with declassification upon completion of the travel.

b. DOD Directive 2000.12 (implemented by SECNAVINST 3300.2A) directs that travel itineraries of DON flag and civilian equivalents be considered at a minimum "For Official Use Only" (FOUO), when their travels take them through high threat countries. These detailed itineraries consist of arrival and departure times, locations of meetings, etc. NCIS reporting that contains such information should similarly be regarded as FOUO.

35-23. INVESTIGATING A THREAT.

a. Whenever there are indications of a credible threat to a DON HRB, an investigation will be conducted using case category 7E (Extortion) for communicating a threat. The investigation will focus on the specific threat in question and will examine issues that impact upon the safety of the principal.

b. NCISHQ Code 21B will be notified of the specific threat and will refer it to the cognizant NCIS field office for investigation. The investigating field office will also notify the NCISHQ Threat Management Unit (TMU) to coordinate investigative efforts. Category 7E cases involving a threat to a principal will be designated as Priority (I) and/or Special Interest (SI) investigations and will require expeditious handling by the cognizant field office.

c. In any instance where a NCIS component becomes aware of a threat to a person protected by the U.S. Government, regardless of agency, such information will be immediately forwarded to Code 21B (Attention: Protective Intelligence). If any reporting is initiated by the local NCIS component, Protective Operations (Code 21B) will be included in the SSD distribution.

35-24. PROTECTIVE COUNTER-SURVEILLANCE.

(b)(7)(E)

b. Reporting on protective counter-surveillance will be accomplished through routine 9A ROI (OPEN), ROI (ACTION), ROI (INTERIM), and/or ROI (CLOSED) either independently or in conjunction with the reporting on a Protective Service Detail.

35-25. TEAM MEMBER DEMEANOR.

a. Protection personnel must become knowledgeable of the individual to whom they are tasked to provide protective support. This would include learning the behaviors, patterns, and likes/dislikes of the principal.

b. Protective personnel must have strong interpersonal skills and the ability to converse and establish rapport with a wide variety of people that they encounter (other law enforcement agencies, military personnel, site managers, etc.) Protective personnel must be able to work out various logistical requirements, often between multiple agencies or organizations.

c. Personnel should not initiate casual conversation with the principal, but should respond politely and concisely if spoken to. Protective personnel will avoid smoking, chewing tobacco, chewing gum, unnecessary talking or other actions that draw undue attention to themselves or the protective operation, or creating a bad impression of the principal.

d. While participating in protective operations, press coverage should always be anticipated and personnel should anticipate that their every move might be subject to exposure by the media, as well as the general public. With the increased use of video cameras, video surveillance and other technologies, protective personnel must act as if every move they make is being recorded. Personnel must exercise a considerable amount of discretion, self-control/restraint and tact in dealing with the media and the public in general.

35-26. TEAM MEMBER EQUIPMENT AND ATTIRE.

a. The minimum necessary equipment to accomplish a protective operation includes:

(b)(7)(E)

b. Vehicles used in protective operations must be maintained in proper fashion. When preparing for protective missions, it is important to ensure that vehicles are clean (inside and out) and all equipment (safety, lights/siren, radios) work properly. Due to the demanding nature of protective driving, it is incumbent on the assigned protective drivers to ensure that proper and routine maintenance is performed on their vehicles. NTAV often have specific scheduled maintenance that occurs more frequently.

(b)(7)(E)

e. Personnel assigned to protective operations should normally be attired in a manner similar to their principal. There will be occasions when the clothing style may vary to casual or formal attire, in which case, the protective personnel must adjust to the situation. When supporting other agencies in protective operations (Army CID PSU, Department of State, USSS), personnel will follow the attire requirements outlined by that agency.

f. Physical fitness clothing and footwear should be routinely available to support protective operations during the principal's physical fitness sessions.

35-27. PROTECTIVE SERVICE PINS.

a. NCIS personnel are issued Protective Service pins along with their badge and credentials. These are serialized, accountable items for inspection purposes and personnel should have their pins accessible during the course of protective missions. Pins are six sided with a small NCIS badge and issued in blue, green, white, and red backgrounds.

b. A primary purpose of the pins is to identify fellow NCIS personnel when working large details and special events that cover large or multiple areas of responsibility (such as the annual

Army/Navy game). The pins are also used to identify NCIS personnel to other protective details that are operating in the same area at the same time. During site advances, the advance team will determine what other protective detail(s) will be in the area, what their pin looks like and what color the other protective detail will be using on the day of the event.

c. In addition to permanent protective service pins, temporary identification pins may be used for large events to identify support, hospitality, security, and other law enforcement personnel. Listed below are some of the temporary pin types used by some key Federal agencies:

United States Secret Service (SARGE)	S – Support Personnel A – Airport Personnel R – Residence Personnel G – Guests E – Enforcement Personnel (armed)
Diplomatic Security - Department of State (WHIPT)	W – Armed Personnel H – Hotel Residence Staff I – Interior Staff P – Press T – Transportation Personnel
United States Marshal's Service (BUCKX)	B – Support Personnel U – Uniformed Armed Personnel C – Airport Personnel K – Authorized Visitors X – Hotel or Residence Staff

35-28. REPORTING.

a. The case category used for NCIS protective operations is category 9A (Protective Services). Case category 5V (Vulnerability Assessment) will be used for reporting PSVAs.

b. Standardized reporting formats for category 9A Protective Services reports capture statistical data that is used to measure various requirements and resources associated with the protective operations mission. As program Manager for all DON protective service efforts, Code 21B must compile accurate protective mission statistics that reflect agency resources devoted to this mission. Any category 9A report will include Code 21B in the Electrical Distribution and Distribution fields of the SSD, and will follow the revised formats noted below.

c. Protection efforts supporting all of the principal's local movements, any events and all travel will be documented via ROI (CLOSED) using the standard 9A format below. The mandatory section titles listed in this report should be in all capital letters, with the corresponding descriptions in upper and lower case italic letters.

REQUESTOR:	*Who requested the protective operations – NCIS, Army CID, DS, USSS, DFLO, etc.*
PRINCIPAL:	*Principal's name, rank/position*
TITLE:	*Principal's title*

COUNTRY:	*Principal's country of origin*
LOCATION:	*City and state or country for the location of the protective operation*
START:	*DDMMMYY for start of mission or special event*
END:	*DDMMMYY for end of mission or special event*
HOURS:	*Total hours to include preparation time, operation and travel of all NCIS personnel supporting the mission from the reporting office*
NCIS EXPENSE:	*Amount of any NCIS expenses, such as travel costs, etc. (excludes C&CI) – format as $00.00*
C&CI EXPENSE:	*Amount of any C&CI expenses– format as $00.00*
PSA:	*Personal Security Advisor, agency and office code*
TEXT:	*Free text area to describe incidents not separately reported, accidents, medical issues, etc. If nothing of interest to report, indicate "Nothing to report."*

PARTICIPANTS
Name, title and office/agency of all law enforcement/security personnel involved in supporting the operation

d. A category 9A Special Operation (9ASO) will be initiated on all principals to which NCIS has assigned a PSA. The 9ASO will document all efforts expended in support of protecting the principal. This umbrella operation will reference all protective support to include: briefings; protective countersurveillance; Protective Intelligence products; PSVAs; and threat investigations, as well as all movements, events and travel reported via the standard 9A ROI (CLOSED) format. Personnel, manhours and funding devoted to the protective operations mission will also be reported in the 9ASO.

e. The 9ASO will be opened as soon as NCIS begins providing protective support to the principal. A 90-day reporting requirement will be used for the 9ASO, in order to capture complete statistics on a quarterly basis. The 90-day reporting timeline requires that ROI (INTERIM) reports be completed after the end of each fiscal quarter, usually within the first two weeks of the new quarter. The ROI (INTERIM) will reference all protective efforts, and summarize the total missions, manhours, personnel and funding expended under this protection operation on the principal over the previous quarter. The format below should be used for the ROI (INTERIM) on 9ASO reports.

EXECUTIVE SUMMARY
1. Summarize total missions performed over the quarter, and the total NCIS personnel used; total NCIS manhours; total NCIS funds; and total C&CI funds used over the quarter.

NARRATIVE
1. Local missions: List number of local missions and break down statistics to reflect NCIS manhours, NCIS funds, C&CI funds and NCIS personnel used over the reporting period to support them.

2. CONUS missions: List number of CONUS missions and break down statistics to reflect NCIS manhours, NCIS funds, C&CI funds and NCIS personnel used

over the reporting period to support them.

3. OCONUS missions: List number of OCONUS missions and break down statistics to reflect NCIS manhours, NCIS funds, C&CI funds and NCIS personnel used over the reporting period to support them.

4. Report miscellaneous text in this paragraph.

f. Protective operations missions in support of SECDEF, DEPSECDEF, CJCS, VCJCS and the Defense Foreign Liaison Office (DFLO), will be initiated and controlled by the Code 21B via 9A ROI (OPEN), and tasking will be set forth via ACTIONS to the affected NCIS Field Offices. NCIS offices will report the results of their tasking by 9A ROI (ACTION) or 9A ROI (CLOSED) as appropriate.

g. All incidents involving the principal, the official party or the protective team will be immediately reported to Code 21B via the most expeditious means possible.

h. Missions in support of the USSS, Diplomatic Security (State Department) or other non-DOD agency should be reported via 9A ROI (CLOSED) using the standard protective mission statistics format.

35-29. TRAINING.

a. NCIS Protective Operations is responsible for providing requirements to the NCIS Training Department (Code 10B) to develop training programs that addresses familiarization training, baseline training, and refresher in-service training. Familiarization training will be provided during the Special Agents Basic Training Program (SABTP) by NCIS Training Department instructors. This training is intended as a basic introduction to protective operations and the methodology that NCIS uses for these missions.

b. Baseline training will primarily be provided at the NCIS Protective Service Operations Training Course at the Federal Law Enforcement Training Center.

c. Follow-on, specific training has variety, and may include driving, shooting and comprehensive schools, such as mission-specific high-risk environment training. All skills and methods taught in the various training venues must be applied within the framework of NCIS policy and regulations.

d. Refresher in-service training will be conducted by NCIS and will be designed for NCIS Special Agents who have completed the Army Protective Services Training Course, the NCIS Protective Operations Training Program, the former NCIS Special Protection Antiterrorism Seminar (SPATS), or who have considerable protective operations experience.

e. All PSAs must complete a baseline protective operations course. Further, it is desirable that the PSA be trained in Advanced First-Aid and CPR. Exceptions to these requirements must be approved in advance by NCISHQ (Code 21B). All protective operations training will be coordinated between Code 21B and Code 10B.

f. NCIS Special Agents traveling with weapons should note approval/transport requirements of the U.S. Federal Aviation Administration (FAA) and the Transportation Security Administration (TSA). See NCIS-1, Chapter 34 for specific details and guidance.

g. NCIS personnel assigned to protective operations must be current with agency qualifications with their assigned/approved duty weapon(s) and the NCIS approved shotgun.

APPENDIX 1: GLOSSARY OF TERMS

Advance Car	Security vehicle that precedes the motorcade by usually 15-45 minutes to ensure that the route to be taken and the destination are free of hazards (such as traffic, construction, etc.) and considered safe for transit.
Advance or Advance Survey	General terms applied to all security activities, plans and arrangements made prior to and in connection with the visit of a principal to a given area.
Command post	Primary field-based operation control center, which coordinates all protective operations support activities in support of a principal. (Formerly called the control room, but changed to be consistent with other agencies.)
Counter-surveillance	Active measures designed to determine if a principal is under surveillance by a potential hostile entity.
Detail Leader	NCIS Special Agent who has responsibility for overall conduct of a Protective Operation. If a PSA is assigned, the PSA will be the Detail Leader. The Detail Leader is responsible for the overall conduct of the mission; however, the Shift Leader has the tactical control of the mission as it occurs. May be called a Detail Agent in Charge by other agencies.
DFLO	Defense Foreign Liaison Office. (See relevant section in text of chapter).
Exigent Circumstances	An issue demanding immediate attention or action. Examples would be an unforeseen request from another agency that is time sensitive or a condition that might result in a threatening situation.
Follow Car	Security vehicle immediately following the principal's vehicle. Whenever practical, a high-rise sports utility vehicle (SUV) will be used. A SUV allows for an excellent observation platform for traffic and surrounding areas and provides room for the evacuation of the principal if needed. (Previously called a Chase Car – terminology was changed to be consistent with other agencies.)
Fully Armored Vehicle (FAV)	Fully armored non-tactical vehicles used to protect occupants from attack by bombs, improvised explosive devices, grenades and high velocity small arms projectiles. Also called a Heavily Armored Vehicle.
High-Risk Billet	Billet designated by the Chief of Naval Operations (CNO-N34) as being at a high level of risk/vulnerability to criminal or terrorist targeting.
Holding Room	Secure area at visit site, usually a private room set aside for the principal's convenience and privacy.
Lead Car	Security vehicle in a motorcade that is immediately in front of the principal's vehicle.
Light Armored Vehicle (LAV)	Non-tactical motor vehicles obtained through normal procurement channels to fill valid transportation requirements and which are later altered by affixing armoring materials to the windows and body areas. LAVs are less than fully armored and are intended to protect occupants from attack by medium velocity small arms projectiles and at least some types of improvised explosive devices. Sometimes referred to as "kit cars."

Motorcade	Formally organized group of motor vehicles traveling along a specified route in a controlled formation.
NFLO	Navy Foreign Liaison Office. (See relevant section in text of chapter).
Personal Security Advisor (PSA)	NCIS Special Agent assigned to a principal, who is responsible for coordinating all protective support to the principal. May be referred to as the "Detail Agent in Charge (AIC)" by other details or agencies.
Personal Security Vulnerability Assessment (PSVA)	Uniform, empirical process developed by NCIS that determines the level of risk and vulnerability of a billet or individual to criminal or terrorist activities. Components include a field-conducted Threat Matrix Questionnaire, NCISHQ Seat of Government (SOG) Inquiries and a PSVA Executive Summary.
Principal	The individual for whom protection is being provided.
Limousine	The vehicle designated to carry the principal.
Protective Operations	All security measures taken to identify threats or vulnerabilities to and/or provide security for the principal.
Protective Service Detail	Team of specially trained NCIS Special Agents assigned to provide a specific level of protective operations support to a principal when a credible threat is present.
PSVA Executive Summary	Written NCIS report that summarizes the results of the PSVA process and provides recommendations for improved personal security.
Route Survey	Selection of primary and alternate routes of travel for the principal and the measures taken to ensure the route is secure for travel.
Safe Haven	A temporary location where a principal may be secured during an attack or threat of imminent attack.
Secure Area	Location that has been examined, cleared of unauthorized persons, and is continuously secured by establishing post assignments prior to use. Certain sites, depending on the nature and location, may also be subjected to electronic sweeping.
Security Perimeter	Placement and utilization of security personnel, alarms, barricades or other devices to provide physical protection, surveillance and intelligence information. These measures are usually associated with a Protective Service Detail.
Security Post	Area of responsibility established to form a part of the protective network, which may be fixed or mobile. Generally, there are three types: surveillance, checkpoint, and special assignment.
Security Room	Similar to a command post, but utilized as the immediate control center for a specific detail or location. The security room may be temporary or permanent and may be used as a squad room for agents not on post. Sometimes assigned a code name and at times is referred to as a command post because of its similar functions on a smaller scale. Usually associated with a Protective Service Detail.
Shift Leader	NCIS Special Agent who has supervisory responsibility on a specific shift or for a specific locale.

Site Survey	Inspection of a given location for the purpose of determining what security measures should be taken for that location. Examples are hotels, banquet halls, conference sites, etc.
Standard Operating Guidelines (SOG)	Detailed plan developed at the local Field Office level that delineates roles and responsibilities of personnel assigned to provide protective operations support to a principal.
Threat Management Plan	Plan implementing the recommendations of the PSVA.
Threat Matrix	Initial stage of a PSVA that consists of a comprehensive survey of significant aspects of an individual's daily life to identify vulnerabilities to criminal or terrorist violence.

Page 1086 redacted for the following reason:
- - - - - - - - - - - - - - - - - - - -
(b)(7)(E)

APPENDIX 3: REFERENCES

1. UNITED STATES CODE (http://uscode.house.gov/search/criteria.shtml)

a. 3 U.S. Code Sec. 202 “United States Secret Service Uniformed Division; establishment, control, and supervision; privileges, powers, and duties”

b. 5 U.S. Code Sec. 303 “Oaths to witnesses”

c. 10 U.S. Code Sec. 1585 “Carrying of firearms”

d. 10 U.S. Code Sec. 7480 “Special agents of the Naval Criminal Investigative Service: authority to execute warrants and make arrests”

e. 18 U.S. Code Sec. 112 “Protection of foreign officials, official guests, and internationally protected persons”

f. 18 U.S. Code Sec. 1114 “Protection of officers and employees of the United States”

g. 18 U.S. Code Sec. 1116 “Murder or manslaughter of foreign officials, official guests, or internationally protected persons”

h. 18 U.S. Code Sec. 3056 “Powers, authorities, and duties of United States Secret Service”

i. 22 U.S. Code Sec. 2709 “Special agents of the Department of State”

2. DEPARTMENT OF DEFENSE DIRECTIVES AND INSTRUCTIONS (http://www.dtic.mil/whs/directives/)

a. DOD Directive 2000.12 "DoD Antiterrorism (AT) Program"

b. DOD Handbook O-2000.12-H “DoD Antiterrorism (AT) Handbook”

c. DOD Instruction 2000.16 “DoD Antiterrorism Standards”

d. DOD Directive C-4500.51 “DoD Non-Tactical Armored Vehicle Policy”

e. DOD Directive 4500.54 “Official Temporary Duty Travel Abroad”

f. DOD Instruction 5030.34 "Agreement Between the United States Secret Service and the Department of Defense Concerning Protection of the President and Other Officials”

g. DOD Directive 5210.56 “Use of Deadly Force and the Carrying of Firearms by DoD Personnel Engaged in Law Enforcement and Security Duties”

h. SECDEF Memo 202200ZMAR95 “Non-Tactical Armored Vehicle (NTAV) Policy Update”

3. DEPARTMENT OF NAVY DIRECTIVES AND INSTRUCTIONS
(http://neds.daps.dla.mil/)

a. SECNAVINST 3300.2A “Department of Navy Antiterrorism/Force Protection (AT/FP) Program”

b. SECNAVINST 5500.29C "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"

c. SECNAVINST 5430.107 “Missions and Functions of the Naval Criminal Investigative Service”

d. OPNAVINST 3300.53 "Navy Combating Terrorism Program"

e. OPNAVINST 3300.54 “Protection of Naval Personnel and Activities Against Acts of Terrorism and Political Turbulence”

f. OPNAVINST 3300.55 “Navy Combating Terrorism Program Standards”

g. MCO 3302.1C “The Marine Corps Antiterrorism/Force Protection (AT/FP) Program”

h. MCO 5500.6F “Arming of Security and Law Enforcement (LE) Personnel and the Use of Force”

i. MCO P5580.2 “Marine Corps Law Enforcement Manual”

Page 1089 redacted for the following reason:
- - - - - - - - - - - - - - - - - - - -
(b)(7)(E)

CHAPTER 36
TITLE: ELECTRONIC INTERCEPTIONS AND ELECTRONIC INVESTIGATIVE AIDS
POC: CODE 00L
DATE: DEC 08

POLICY DOCUMENTS:

Appendix (7) Gen Admin 11C-0011 of 24 March 2014 released Policy Document number 14-02 Operational (Consensual Interceptions for Law Enforcement Purposes (FOUO-LES). Policy document 11C-0011 contains new or revised policy that has not been incorporated into this chapter and should be reviewed in its entirety.

36-1. GENERAL. This chapter addresses the interception of oral, wire, and electronic communications for law enforcement purposes; the use of pen registers, and trap and trace devices for law enforcement purposes; the use of tracking devices and closed circuit television (CCTV) for law enforcement purposes. For definitions of terms used throughout this chapter, see Appendix (1).

36-2. LAWS AND REGULATIONS

36-2.1. The use of electronic interception devices, pen registers, and telephone tracing devices for law enforcement purposes is regulated by statute and Department of Defense (DoD) regulation. Law enforcement use of video-only CCTV is not regulated by statute or DoD regulation, but is subject to the Fourth Amendment proscription against violating a person's reasonable expectation of privacy without a court order. The use of tracking devices is addressed in Title 18 United States Code (USC) Section 3117 and is subject to Fourth Amendment proscription against violating a person's reasonable expectation of privacy.

36-2.2. The ECPA, Title 18 USC Sections 2510-22, 2701-11, and 3121-27.

a. The ECPA updated the Wiretap Act of 1934 and Title III of the Omnibus Crime Control and Safe Streets Act of 1968. The ECPA is divided into three titles: Title I (Sections 2510-22) governs the interception of oral, wire, and electronic communications for law enforcement purposes; Title II (Sections 2701-12) governs access to stored electronic communications; and, Title III (Sections 3121 and 3127) governs the use of pen registers and trap and trace devices.

PRACTICE NOTE: Law enforcement officials and prosecutors will often refer to court orders for the nonconsensual interception of oral, wire, and electronic communications as "Title III's". For example, if a prosecutor says, "we'll need a Title Three for that", they mean that a court-order will be required for a nonconsensual interception. This is a reference to Title III of the Omnibus Crime Control and Safe Streets Act of 1968. Technically, such a statement is inaccurate, as the nonconsensual interception is now governed under Title I of ECPA. In fact, some prosecutors and law enforcement officials now refer to nonconsensual interception orders as "Title One's". Be aware that a speakers' reference to "Title One" or "Title Three" mean the same thing: a court order for nonconsensual interception. Special agents should be aware that nonconsensual intercepts can be manpower intensive.

b. Section 2511 sets forth the criminal penalties for conducting nonconsensual interceptions of oral, wire, or electronic communications without a court order. This law does not prohibit interceptions where one party to the communication consents to the interception. Procedures for obtaining a warrant to conduct nonconsensual interceptions for law enforcement purposes are set out in Title 18 USC Section 2518. Nonconsensual oral and wire interceptions (but, not electronic interceptions) are also governed by Title 18 USC Section 2516, which requires that a Department of Justice (DOJ) official, no lower than Deputy Assistant Attorney General, authorize any application to a federal judge for an oral or wire interception.

36-2.3. DoD Directive 5505.9 of 20 April 1995, Subject: Interception of Wire, Electronic, and Oral Communications for Law Enforcement; and DoD Directive O-5505.9-M of May 1995, Subject: Procedures for Wire, Electronic, and Oral Interceptions for Law Enforcement.

a. These regulations govern the use of electronic aids for law enforcement purposes within DoD. There is no implementing Department of the Navy (DON) instruction. The DoD directive and manual implement ECPA and regulate nonconsensual and consensual interceptions, pen registers, and trap and trace devices for law enforcement purposes only. The DoD directive and manual are

applicable both in the U.S. and abroad. The manual also controls the storage, inventory, and use of interception information.

NOTE: Under these DoD regulations, use of consensual interceptions for law enforcement purposes within DoD can be conducted only by defense criminal investigative organizations, i.e., Defense Criminal Investigative Service (DCIS), NCIS, United States Army Criminal Investigation Command (USACID), and Air Force Office of Special Investigations (AFOSI). Stated differently, local commands, military police, base security, Marine Corps CID, inspectors general, etc., are not authorized to conduct consensual interceptions.

36-3. APPLICATION OF THE LAWS AND REGULATIONS TO NCIS LAW ENFORCEMENT OPERATIONS

36-3.1. If NCIS is solely conducting a law enforcement operation within the United States, as it concerns intercepting oral, wire, and electronic communications, NCIS must comply with ECPA and the DoD regulations. If the operation will involve interceptions overseas, NCIS must also comply with local foreign law and any applicable Status-of-Forces Agreement (SOFA) or other treaty between the U.S. and the host nation.

36-3.2. Joint Law Enforcement Operations With Other Federal Agencies. In joint operations conducted with another federal law enforcement agency, either agency can obtain authorization to conduct intercepts. In cases where NCIS and another DoD law enforcement agency (i.e., AFOSI, USACID, DCIS) are conducting a joint investigation, the lead agency will be responsible for obtaining interception authority according to their respective service rules. Duplicate authority is not needed and discouraged. The use of electronic interceptions in these operations, however, will be reported in the periodic Report of Investigation (ROI) submitted by the NCIS case agents. The closed investigative case file should be sent to the Records Management Branch (RMB) (Code 11C1), Administrative and Logistics Directorate, for retention and indexing.

36-3.3. Joint Law Enforcement Operations With State, Local, or Foreign Agencies. When NCIS is a partner in a joint criminal investigation with law enforcement personnel of a state, local or foreign agency, in which electronic interceptions or pen registers conducted for law enforcement purposes are to be conducted, the requirement to obtain DON authority, and other requirements under DoD Directive 5505.9 as explained in this chapter, apply whenever there is a DON interest in the investigation (if no DON interest, NCIS should not be participating in the investigation). DON interest exists in the interceptions in such a joint criminal investigation whenever any one or more of these circumstances is present:

a. A NCIS special agent, a member of the naval service, any DON employee, or property under DON control is outfitted with electronic interception equipment; or,

b. The target of the interception is a member of the naval service or an employee of the DON; or,

c. The interceptions may take place on DON controlled property.

36-3.4. If there are any questions, contact the Staff Judge Advocate, NCIS Legal Office (Code 00L) for assistance.

36-3.5. Any violations of the policy reflected in this chapter, must be reported via telephone and in writing to Code 00L via the appropriate NCIS field office Special Agent in Charge (SAC) or Deputy Assistant Director (DAD), and reflected in an appropriate report; see Section 36-8.

36-4. REQUESTING INTERCEPTION AUTHORITY FOR LAW ENFORCEMENT PURPOSES - GENERAL

36-4.1. Except under exigent circumstances, whenever a NCIS special agent desires to use consensual interception or is involved with its use as noted in section 6-3.3, authority must be obtained from the Director, NCIS. To obtain authority from the Director, the special agent submits a ROI to their SAC, or designated Acting SAC, for review and submission to Code 00L. The request must contain the approving official by name and office (i.e., SA John Doe, SAC, Southeast Field Office has reviewed and concurs with this intercept request.) The request will then be processed for authorization by the Director, NCIS or his Acting designee. Section 36-6 and subsequent paragraphs set out procedures for various kinds of interception authority.

36-4.2. Under exigent circumstances, verbal authorization may be obtained from the Director, NCIS. However, all verbal requests, due to exigent circumstances, must be made through the respective Supervisory Special Agent (SSA), Assistant Special Agent in Charge (ASAC) or SAC, and Code 00L. In rare situations, in which use of consensual interception must be immediately undertaken to protect human life under circumstances in which timely verbal authorization from NCISHQ cannot be obtained, use of consensual interception may be authorized by the senior special agent on scene. In either case, all verbal requests must be immediately followed-up with a written request within 24 hours.

NOTE: An example in which such use could be authorized by the senior special agent would include the early stages of a hostage situation. It would not include the situation in which a cooperating witness (CW) informs a special agent that the CW could make an immediate purchase of narcotics from a drug dealer.

36-4.3. After-Hours Consensual Intercept Requests.

a. Consensual intercepts are a valuable investigative tool and should be used whenever practical, but proper planning and timely submissions are essential. The Director, NCIS, or in his absence, an individual designated as Acting Director, is the only individual authorized to approve requests for consensual intercepts. The Director is available during normal business hours (Eastern Standard Time). Under normal circumstances, an intercept request should be transmitted to Code 00L during normal business hours. Code 00L will perform the required legal review and present it to the Director, NCIS for authorization. Even "routine" requests are handled expeditiously.

b. Only in extraordinary circumstances should after-hours requests be submitted via telephone to NCISHQ personnel at home. There are certain rare situations in which after-hours requests cannot be avoided, such as when a unique opportunity to obtain essential evidence will be lost if an intercept is not conducted expeditiously.

c. In those extraordinary cases, the NCISHQ attorneys may be contacted via telephone (residence or mobile). No after-hours requests should be made to a paralegal. Current attorney contact information is available from the NCIS Multiple Threat Alert Center (MTAC) Watch Center at (b)(6), (b)(7)(C) The attorney will process the oral request, provide a legal

review and contact the Director, NCIS to obtain oral approval. If approval is given, the attorney will inform the requesting agent, who must follow up with a ROI (ACTION) on the next business day.

36-4.4. Central Point. The NCISHQ central point for coordinating consensual interception authorizations is the NCIS Staff Judge Advocate's (SJA) Office, Code 00L. Code 00L coordinates with other NCIS codes as appropriate.

36-4.5. Local Laws. Before a special agent considers the use of electronic interception devices, local laws should be considered. While a local state law within the U.S. may not affect the use of electronic interception device by the NCIS special agent, it can prohibit the later introduction of the interception results in the state criminal trial. Also, outside the U.S., host nations often are more restrictive about the use of electronic interception devices than the United States.

a. For example, the use of electronic interception devices is greatly restricted in the Philippines. Use of such devices by a special agent could result in his/her legal detention or confinement. Always be aware of local, state, and foreign laws before using electronic investigative aids. If there are questions, contact a local Judge Advocate General (JAG) or Code 00L for advice.

36-5. NONCONSENSUAL INTERCEPTIONS

a. Within the United States. In general, nonconsensual interceptions of oral, wire, and electronic communications (including the audio portion of a video/audio recording), conducted within the United States for law enforcement purposes, are permitted only after a court order has been obtained, in accordance with Title 18 USC Section 2518, and only to further investigations of those offenses enumerated in Title 18 USC Section 2516. NCIS special agents seeking a court order for nonconsensual interceptions should liaison with NCISHQ Codes 00L and 24B1 (for equipment), and if the intercept involves computer communications, NCISHQ Cyber Department, Code 24D. Interception orders are typically obtained in Federal District Court, so the special agent will also have to work closely with the cognizant Assistant United States Attorney (AUSA).

36-6. REQUESTING CONSENSUAL INTERCEPTIONS

36-6.1. Offenses. To conduct a consensual interception at least one of the parties to the conversation must have given advance consent and the investigation must involve:

a. A felony offense; or

b. Telephone calls to DoD installations, facilities, buildings, or residences of DoD personnel, which convey obscene information, undue harassment, bomb threats, threats of other bodily harm, offers of bribery, or attempts at extortion.

36-6.2. Form Of Consent. Consent must be obtained in writing from the consenting individual, except in the case of federal, state and local law enforcement officers, in the format contained in Appendix (2). Attach the written consent as an attachment to the appropriate ROI.

36-6.3. The Request. When an special agent wants to conduct or take part in a consensual electronic interception, a ROI, approved by the SAC or his/her Acting designee, is submitted to Code 00L, info to NCIS Codes 21, 22, 23, and/or 24 as appropriate. Code 00L then submits a memorandum to the Director, NCIS with the request to conduct or participate in a consensual electronic interception investigation. Subsequent to the Director's approval, a ROI (ACTION) will be sent to the requesting agent with information copies to affected supporting offices and respective NCISHQ Codes. The ROI request for consensual interception of wire, electronic, or oral communication shall include the following:

a. A reasonably detailed statement of the background and need for the interception and the nature of the evidence sought.

b. A citation of the applicable federal, state, foreign statute, or provision of the Uniform Code of Military Justice (UCMJ).

c. If an interception is for protection purposes, the request must explain the danger to the consenting party.

d. A general description of the type of device(s) to be used and the location, i.e., on the person, in personal effects, or in a fixed location.

e. A particular description of the nature and location of the facilities from which, or the place from where, the communication is to be intercepted. In the United States, the request must include reference to the primary judicial district where the interception will take place for targets not subject to the UCMJ or if known, the convening authority for targets subject to the UCMJ.

f. The length of time needed for the interception. Initially, an authorization may be granted for up to 90 days from the day the interception is scheduled to begin. Extensions may be granted for periods of up to 90 days. In special cases, such as targeting narcotics sales sites, fencing or undercover operations, authorization for up to 180 days may be granted with similar extensions.

g. The name of the consenting party. Names of undercover operatives, cooperating citizens, or informants may be identified by an individualized informant or source control number. If consent was not obtained in writing, submit a statement explaining how consent was obtained.

h. Names, when known, of non-consenting parties whose conversations are expected to be intercepted, or who are otherwise to be monitored, and their roles relative to the offense being investigated.

i. A statement that the facts of the interception have been discussed with the cognizant prosecuting attorney and that such attorney has indicated (orally or in writing) the interception is appropriate. If the target of the investigation is subject to the UCMJ, the statement of facts shall be discussed with and approved by a judge advocate with the appropriate functional responsibilities. The NCISHQ SJA is available for consultation.

j. The interception has been reviewed by the SAC, or in the absence of the SAC, the designated

Acting SAC. The request must contain the approving official by name and office (i.e., SA John Doe, SAC, Southeast Field Office has reviewed and concurs with this intercept request).

k. A request for renewal must refer to all previous authorizations and explain why an additional extension is required. If the authority was not used an explanation must be provided.

36-7. INTERCEPTIONS REQUIRING DOJ APPROVAL

36-7.1. Written authorization from the DOJ OEO shall be obtained when it is known that:

a. The interception relates to an investigation of a Member of Congress, a federal judge, a member of the Executive Branch at Executive Level IV or above, or a person who has served in such capacity within the previous two years; or,

b. The interception relates to an investigation of the governor, lieutenant governor, or attorney general of any state or territory, or a judge or justice of the highest court of any state or territory, and the offense investigated is one involving bribery, conflict of interest, or extortion relating to the performance of his or her official duties; or,

c. The interception relates to an investigation of a federal law enforcement official; or,

d. The consenting or non-consenting person is a member of the diplomatic corps of a foreign country; or,

e. The consenting or non-consenting person is or has been a member of the Witness Security Program and that fact is known to the agency involved or its officers; or,

f. The consenting or non-consenting person is in the custody of the Bureau of Prisons or the U.S. Marshals Service; or,

g. The Attorney General, Deputy Attorney General, Associate Attorney General, Assistant Attorney General for the Criminal Division, or U.S. Attorney for the district where an investigation is being conducted has requested the investigating agency obtain prior written consent for making a consensual interception in a specific investigation.

36-7.2. It is imperative that as much lead-time as possible be given in these matters. A two-to-five day lead-time is reasonable. Proper planning and early consideration of this technique will permit handling of this matter by submitting a ROI. While last minute requests to obtain permission from the Director, NCIS are possible, they should be reserved for emergency or exigent circumstances. Code 00L staff encourages telephonic consultation regarding intercept matters.

36-8. FIELD REPORTING REQUIREMENTS

36-8.1. Report After Use. When an oral or wire interception has been conducted as part of an investigation, the details will be submitted by ROI to Code 00L. The report must include the following:

a. The interception activity must be identified accurately, such as a "consensual oral interception", "consensual wire interception", or, "consensual electronic interception"; and,

b. The dates of the interceptions; and,

c. The locations of the interceptions; and,

d. The full identity of individual(s) who have been intercepted or recorded; and,

e. A brief summary of the results of the interception; if the authority was not used a short explanation as to why the authority was not used; and,

f. Any deviation from the information given in the requesting ROI (such as different equipment used) must be included and clearly set forth; and,

g. The storage location of any tapes or transcripts of interception activity.

36-8.2. ROI Reporting. If a timely ROI was not used to submit a report of the use of electronic interceptions in the investigation, a brief summary of the results of the interception must also be included in the next ROI on the case along with the name of the authority who authorized the interception (e.g., Director, NCIS).

36-8.3. Timely Reporting Requirements. No extensions of interception authority will be given until a report on the last period of authority is received. Reports, in ROI format, are due no later than the 10th working day from the last day that the authority then being used was in effect.

36-8.4. Should the interception operation overlap two calendar quarters, an interim report with the information in subparagraph 36-8.1 above is required. Calendar quarters end on 31 March, 30 June, 30 September, and 31 December. Reports should be received by the fifth working day following the end of the quarter.

36-8.5. Monthly Reports. In cases of special operations where there is no single person identified for interception, such as in drug suppression operations or sting operations, reports must be submitted on a monthly basis. These reporting requirements are imposed by outside authority and must be met. Failure to meet them could result in curtailment of this technique.

36-8.6. Reporting Joint Federal Operations. Joint operations conducted with another federal agency, where the other federal agency obtains authority, must be reflected in the ROI covering the period of the interception. The ROI must reflect the source of the other agency's interception authority (i.e., AUSA Jane M. Doe, Southern District of New York.)

36-8.7. Other Information. NCISHQ prepares responses to requests of disclosure, made in connection with military and civilian court proceedings, which requires Code 00L to maintain the central file detailing all interceptions conducted by the Navy. This information is usually extracted from the ROI that reports approved NCIS interceptions. One question routinely asked in civilian-

court federal-information requests is whether NCIS files contain any evidence obtained as a result of interceptions conducted by another law enforcement agency. Accordingly, information that NCIS acquires as the result of interceptions conducted by another law enforcement agency should be documented in an ROI, detailing the source of the information and the identity of those individuals whose conversations have been intercepted. Include Code 00L in all reporting distribution. The information will be entered into the computer database to permit an accurate response. This requirement is mandatory and compliance is essential.

36-8.8. Authority Not Used. Where no interceptions have occurred, negative reports must be submitted with a brief explanation as to why the authority was not used.

36-9. DISPOSITION OF INTERCEPTION TAPES AND RECORDS

36-9.1. Consensual Interception Recordings. Consensual interception recordings shall not be forwarded to NCISHQ Code 00L, but rather retained in local evidence lockers and disposed of under the same general rules that apply to the handling of other physical evidence. That is, such recordings shall not be disposed of until:

a. All court actions, trials, and appeals are final.

b. Disposal is approved by an appropriate military judge advocate or, in the case of recordings used for prosecutions in the civilian community, the civilian prosecuting attorney.

(1) Appropriate military judge advocates that can approve the disposition of consensual recordings include:

(a) The trial counsel (or, successor) who prosecuted the case or superior trial counsel; or,

(b) In cases in which a trial counsel was not involved (for example, court-martial charges were not preferred), the local station, base, or command judge advocate; or,

(c) The judge advocate assigned to the NCIS resident agency office holding the recordings; or,

(d) In cases not falling under the above, any judge advocate assigned to NCISHQ.

(2) When authorization for disposal is obtained from the appropriate military judge advocate or civilian prosecuting attorney, the evidence custodian shall complete the final disposition section of the evidence custody document by recording the name and title of the person authorizing the disposal and the date such authorization was obtained.

(3) If transcripts of tape recordings are made, such transcripts shall be included in the permanent case file.

36-9.2. Non-consensual Recordings. All recordings, logs, and transcripts of non-consensual intercept activity must be retained for a minimum of 10 years, and may only be destroyed by court

order. When no longer required for use at the local level, all such recordings, logs, and transcripts shall be forwarded to RMB Code 11C1, for long-term retention and ultimate disposition.

36-10. MINIMIZATION

36-10.1. When conducting electronic interceptions, the NCIS special agent should always endeavor to minimize the unnecessary intrusion into the privacy of parties not involved in the investigation for which the interceptions are being conducted. The special agent must reduce to the smallest practicable extent interceptions of non-pertinent conversations.

36-10.2. Disclosure of Intercepts. The contents of any interceptions should not be disclosed to persons without a need to know.

36-10.3. Code 00L should be consulted concerning the minimization requirements appropriate to non-consensual interceptions.

36-11. RECORDING INTERROGATIONS AND INTERVIEWS

36-11.1. The recording of interrogations by overt video or audio means within the confines of an NCIS facility having the technical capabilities for such recordings shall be accomplished in all investigations involving crimes of violence. Crimes of violence include homicide, sexual assault, aggravated assault, robbery, and crimes involving weapons. A decision not to record may be made by the SAC, or the supervisory designee, when circumstances of investigative environment dictate that recording would be counterproductive or otherwise impede the interrogation.

36-11.2. Supervisory engagement regarding the use of audio or video recording of interrogations is required and shall be documented in the case activity record (CAR). Factors for consideration of whether to record an interrogation are provided in Appendix (3). The factors listed in Appendix (3) should not be considered all inclusive or restrictive.

36-11.3. NCIS components shall adhere to the specified procedures to ensure uniformity of policy administration. It is envisioned that all NCIS components will eventually become technically capable to record interrogations consistent with the guidance provided below:

a. All NCIS field components shall post a warning sign at each entrance to rooms being used for interrogations informing those who enter that they are subject to electronic monitoring. The sign shall read “ROOM SUBJECT TO AUDIO/VIDEO RECORDING AT ALL TIMES”. The sign shall measure 8.5” by 11” at a minimum and be clearly visible to anyone entering the room. Signs shall be produced locally; a sample sign titled “Recording Interrogations Sign” is posted on the NCISnet under Downloads, Forms, and Investigative Forms. Overseas components may post an additional sign in the host country native language but must ensure the translation is consistent with the specific meaning of the above verbiage. If an NCIS office is located in an area where a foreign language is widely spoken, an additional sign may be posted in the respective language.

b. No additional written or verbal notification is needed prior to conducting an interrogation.

c. If the person being interrogated objects to being recorded, the recording equipment shall be immediately turned off and remain off throughout the interrogation and statement taking process.

d. Recording equipment shall be turned off when a person is conferring with their lawyer or with a chaplain. It should be noted on the recording the time the recorder is turned off and restarted.

e. The entire session, except for when a person is conferring with their lawyer or with a chaplain, shall be recorded from the time the person being interrogated enters the room until the time he/she departs, to include the statement taking process.

f. Even if a subject has made a recorded statement, the subject shall be afforded the opportunity to provide a written statement in their own handwriting or prepared for him/her by an agent.

g. The master recording shall be treated as evidence consistent with NCIS policy on evidence processing and a log of copies made shall be maintained in the case file.

36-11.4. Whenever an interview/interrogation is electronically recorded, appropriate annotation of that fact shall be documented in an Investigative Action (IA) and included in the reporting ROI. The ROI shall also distinguish if the recording was video/audio, or just audio. If the decision is made not to record interrogations relating to crimes of violence, the rationale for that decision (e.g., the office interview room not equipped for recording) and the identity of the supervisor making that decision shall be annotated in the CAR. Situations wherein a person specifically objects to being recorded during an interview/interrogation shall also be reported in the ROI.

36-11.5. The master recording shall be maintained as evidence until the case is fully adjudicated including the appeals process. A ROI shall reflect where the recording was placed into evidence, to include the date and evidence log number. A log shall be established to document any reproductions or copies of recordings. The log shall be maintained in the case file and shall reflect the name of the requestor, the date copies were made, and to whom the copies were provided. A copy of the recording shall not be submitted as part of the closed file.

36-11.6. Transcription of recorded interrogations is not the responsibility of NCIS.

36-11.7. Polygraph examinations conducted in support of criminal or counterintelligence investigations will not be audio/video recorded without prior approval of the Chief, Polygraph Services Division (Code 24B2), Operational Support Directorate. Counterintelligence Scope Polygraph examinations are not affected by this change in policy.

36-11.8. Absent exigent or extraordinary circumstances, interrogations of persons involved in crimes of violence shall be conducted with two investigators present, regardless of whether the interrogation is recorded.

36-11.9. During joint investigations in which another agency has primary jurisdiction, the other agency's policy supersedes the requirements set forth in this chapter.

36-11.10. Agents should consider use of this investigative tool in all investigations.

36-12. PEN REGISTERS AND TRAP AND TRACE DEVICES

36-12.1. In the United States.

a. Except when the consent of the user has been obtained, the installation and use of a pen register, or trap and trace device, is permitted only after a court order has been obtained, in accordance with Title 18 USC Sections 3122-23.

NOTE: As a general notice, all users of a DoD telephone system are subject to being monitored and recorded; the use of the telephone is consent to being monitored and recorded, and this is sufficient to support installation of a pen register, or trap and trace, device. Appendix (4) provides a sample banner used in addition to the monitoring statement often found in installation telephone directories.

b. If the consent of the service user has not been obtained, the following procedures shall be used to obtain authorization to use and install a pen register, or trap and trace, device:

(1) An attorney from the local U.S. Attorney's office or from the DOJ shall make application for an order, or an extension of an order, authorizing or approving the installation and use of a pen register, or trap and trace, device, in writing, under oath or equivalent affirmation, to a court of competent jurisdiction.

(2) The application shall include the identity of the attorney making the application, the identity of the law enforcement agency conducting the investigation, and a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

(3) Emergency authorization to use and install a pen register, or trap and trace, device shall be requested per Title 18 USC Section 3125 through coordination with the local U.S. Attorney or the OEO, DOJ.

36-12.2. Outside of the United States. If the target of the law enforcement investigation is subject to the UCMJ and trial by court martial may result, use of a pen register, or trap and trace, device may be approved by a military judge designated by the JAG. Per DoD Directive O 5505.9-M, Chapter 1D.2, the military judge must find that the contemplated use and installation of a pen register or trap and trace device does not violate the law of the host country, any applicable Status of Forces Agreement (SOFA), or any other agreement with the host country. See Appendix (5) for an application for a pen register and Appendix (6) for an order for applying for a pen register.

36-13. LISTENING IN ON EXTENSION LINES

36-13.1. DoD law enforcement personnel are authorized to monitor telephone conversations by listening in on an existing extension telephone, without need for prior approval from higher authority, if at least one party to the conversation consents to such monitoring.

36-13.2. Listening in on extension lines is reported only by mention in the ROI reporting the case.

36-14. MOBILE TRACKING DEVICES IN LAW ENFORCEMENT

36-14.1. With the consent of the person who will wear the beeper, or on whose property the beeper will be attached, there is no requirement for approval by higher authority and no reporting requirement. Beepers mounted in property with the consent of the owner may still be monitored when the property is transferred to a non-consenting party as long as the property does not enter a private area. Written permission of the consenting individual is not required but is encouraged.

36-14.2. When the beeper will be non-consensually mounted (e.g., a slap-on beeper or a surveillance beeper), it may be used without court-order, if it is mounted on property accessible to the public, and the mounting is done in a public location. The beeper may then be monitored as long as the property to which it is attached stays in public areas.

36.14.3. Special agents may place a Global Positioning System (GPS) tracking device on a suspect's vehicle, parked in a public place, without first acquiring a warrant or command authorized search. Note that if the case is to be prosecuted in state court, agents should consult the state prosecutor first, or contact Code 00L, for more specific guidance. The placement of a GPS tracking device is not wiretapping and does not trigger judicial requirements under 18 USC 2518 (Procedure for interception of oral, wire, or electronic communications). NCIS rarely conducts Title III wire-tapping operations. Additionally, placing a GPS tracking device on a suspect's car does not fall under DoD Directive 5505.9 - Interception of Wire, Electronic, and Oral Communications for Law Enforcement, as there is no oral communication to intercept. In the case of US v McIver, 186 F 3d 1119 (9th Cir 1999), the court held that the placement of a GPS tracking device on a vehicle is not an act that triggers the protections and requirements of the Fourth Amendment's warrant clause. In the case of US v. Moran, 349 F. Supp 2d 425 (N.D.N.Y. 2005) the court found that the placement of a GPS tracking device did not violate the Fourth Amendment. The court noted that a person has a diminished expectation of privacy in a vehicle because of its availability to public scrutiny and that the police could have gathered the same evidence (regarding movement of the suspect on roads) through visual surveillance. Citing the case of US v Knotts, 460 US 276 (1983), the court held that a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movement from one place to another.

CAVEAT: It is conceivable that there are situations where a vehicle with a GPS tracking device may leave the public roadway and enter an area not in public view. So long as a vehicle is in a situation where it could be viewed in public, evidence obtained from the GPS tracking device would be admissible in court. Once the vehicle moved into a non-public place that could not be viewed by the public, tracking should cease.

36-14.4. When the nonconsensual mounting or monitoring of beepers and GPS tracking devices is

contemplated, close liaison with Code 00L is strongly suggested.

Warrant Requirements – Installing GPS devices on/in vehicles				
Location **OF** Vehicle during installation	In REP area	Not in REP area	In REP Area	Not in REP area
Location **ON** Vehicle	In REP area (Internal installation)	Not in REP area (External installation)	Not in REP area (External installation)	In REP area (Internal installation)
Officer action	Warrant required.	No warrant required.	Warrant required.	Warrant required.

36-15. VIDEO AND CLOSED CIRCUIT TELEVISION (CCTV)

36-15.1. As a general rule, when the use of video-only (no audio recording) CCTV or other photographic monitoring device is contemplated, a warrant or command authorization is not required, unless the CCTV or photographic device will be monitoring an area where a person enjoys a reasonable expectation of privacy.

NOTE: Special agents are not allowed to commit a trespass to mount the CCTV or photographic device.

36-15.2. When sound is also recorded as a part of a closed circuit or camera monitoring setup, all the rules and authority requirements applicable to the particular kind of electronic sound interception involved apply. For example, if a video camera that not only takes pictures but also records sound is used to take pictures of a drug transaction in a public parking lot, a warrant would not usually be required for the pictures being taken; but, authority or a warrant would be required for the sound being intercepted, depending on whether the interception was consensual or non-consensual.

36-15.3. Reporting. Unless sound interceptions are involved reporting of video or closed circuit television need only be made by ROI. If sound is intercepted, Sections 36-9 and 36-10 apply.

,

36-15.4. When the use of closed circuit television or other photographic surveillance in areas of questionable expectation of privacy is contemplated, liaison with a local attorney or Code 00L is strongly suggested.

36-15.5. Surreptitious use of closed circuit television monitoring for foreign intelligence and counterintelligence purposes is specifically regulated by FISA and DoD 5240.1-R, Procedures 5 and 6.

36-16. CONTROL OF EQUIPMENT

36-16.1. Storage of intercept equipment will be centralized to the maximum extent possible consistent with operational requirements and stored together in a locked container. In order to meet operational needs, intercept equipment will be maintained and controlled by the NCIS Technical Services Detachments. Custody of intercept equipment can thereafter be delegated to the direct

control of a supervisor, designated in writing by the SAC, at each field office, resident agency, or resident unit ensuring that offices have access to intercept equipment. One or two alternate custodians will also be assigned in writing in order to insure that intercept equipment is available when needed. Each time delegated custodial responsibilities are reassigned, a copy of the assignment letter will be forwarded to the local Technical Services Detachment.

36-16.2. Each office will maintain an ongoing "Intercept Utilization Log" to track and account for intercept equipment. This log will, at a minimum, contain the following entries; date removed from storage, date returned to storage, equipment nomenclature, equipment serial number, purpose of withdrawal, applicable NCIS Case Control Number (CCN), printed name of the individual accepting responsibility for the equipment, and the individual's initials. There will only be one log to record the utilization of all maintained intercept equipment for each office. This log will be permanently kept on file. Offices that do not maintain intercept equipment will create an Intercept Utilization Log to record the use of intercept equipment borrowed from other offices. The office loaning the equipment will annotate its log to reflect the office receiving the equipment. The receiving office will record the actual utilization of the equipment. Any time equipment is permanently transferred from one office to another, the local Technical Services Detachment must be notified in writing. This record must be maintained for a five year period. Pages with entries older than five years may be removed from the log and destroyed. A Intercept Equipment Utilization Log may be obtained by contacting the Technical Services Division, Code 24B5.

36-16.3. When equipment is checked out for utilization, the control of the equipment becomes the responsibility of the special agent initialing receipt of the equipment. Equipment may be kept in that special agent's custody for the period of time necessary to complete the intercept(s) or meet operational requirements before being returned to storage. However, a report must be made documenting each use of the equipment during the period of time removed from storage in accordance with Code 00L policy set forth in this chapter. When equipment is in the control of a special agent and not in use, it must be secured and controlled to the greatest extent possible.

36-16.4. An inventory of intercept equipment will be conducted each January. The results of the inventory, along with a photocopy of the previous year's Intercept Utilization Log pages, will be forwarded to the local Technical Services Detachment for reconciliation. After accounting for all intercept equipment, local Technical Services Detachments will report results to the Technical Services Division.

36-17. LAW ENFORCEMENT OPERATIONS IN AN AUTOMATED ENVIRONMENT

36-17.1. Within NCIS, the Cyber Department (Code 24D), Operational Support Directorate, has primary cognizance over law enforcement operations in a computer/electronics environment. Such operations typically involve legal issues that require coordination with Code 00L and the DOJ.

PRACTICE NOTE: An excellent resource on this topic is the DOJ Computer Crimes and Intellectual Property Section booklet "Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations," available at the DOJ Cybercrime Web site.

36-17.2. As noted earlier in this chapter, the ECPA of 1986 restricts:

a. The interception of electronic communications; and/or,

b. Gaining access to stored electronic communications, and/or,

c. Using pen registers, and trap and trace, devices. Electronic communications are defined to include communications between computers and computer networks.

36-17.3. Intercepting Electronic Communications.

a. ECPA updated the Wiretap Act of 1934 and the Omnibus Safe Streets and Crime Control Act of 1968, to include the interception of electronic communications. "Electronic communications" are defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence or any nature transmitted in whole or in part by a wire [read any telecommunications system], radio, electromagnetic, photoelectric, or photo-optical system that affects interstate or foreign commerce" (Title 18 USC Section 2510(12)). In short, ECPA makes it illegal to intercept electronic communications, unless such interceptions are made pursuant to court order or are otherwise permitted under one of the statute's exceptions.

b. This is the law that generally makes it illegal to conduct keystroke monitoring or intercept electronic mail (e-mail) or retrieve e-mail from storage in a file server, unless one of the statute's exceptions apply.

c. The law does allow interceptions, without a court order, under certain exceptions. The following exceptions are noteworthy:

(1) Interceptions lawfully made through the Attorney General under FISA.

(2) Interceptions made with the consent of at least one of the parties to the communication:

(a) The Wiretap Act always permitted the consensual interception of oral and wire communications. Thus, it is lawful for an undercover policeman to wear a body microphone and transmitter to record conversations during a drug deal. Similarly, a law enforcement officer may record a telephone call between the victim of a crime and a suspect if the victim consents to such recording. "Electronic communications" are defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence or any nature transmitter in whole or in part by a wire [read any telecommunications system], radio, electromagnetic, photoelectric, or photo-optical system that affects interstate or foreign commerce" (Title 18 USC Section 2510(12)).

(b) ECPA also permits the consensual interception of electronic communications. This has at least two potential applications for law enforcement activities in an automated environment:

(c) First, ECPA does not prohibit a special agent from intercepting communications between the special agent and another party over a computer network; for example, a real-time computer chat. This includes communications made by the special agent in an undercover capacity and communications made by a source. Authorization must be obtained under Section 36-4.

(d) Second, if a computer or computer network contains a properly worded banner, advising users that use of the computer and/or network constitutes consent to have their communications intercepted, then such communications can be lawfully intercepted under the ECPA, because the users have given their consent to such interception. Authorization must be obtained under Section 36-4. A sample banner is provided, see Appendix (4).

NOTE: All DoD computers and computer systems should be protected by banners, preferably the sample banner as shown in Appendix (4), which is the DoD General Counsel Memorandum, "Communication Security and Information Systems Monitoring," March 17, 1997. If a DoD system is not protected by a banner, the special agent should work with the system administrator to have the banner added. Additionally, all users should have read and signed DD Form 2875, System Authorization Access Request (SAAR), acknowledging that there is no right to privacy in the government system.

(3) Limited authority for System Administrator/System Operator (SYSOP). ECPA permits a SYSOP to monitor the system to the extent necessary to manage the system. The SYSOP may also read the text of e-mail if the originator or the addressee consents (including consent-through-banner). Further, if the SYSOP inadvertently obtains a message and the message appears to pertain to a crime, the SYSOP may disclose the contents of the message to a law enforcement agency. DoD Directive 5505.9, dated 20 Apr 95, and DoD O-5505.9-M, dated May 1995, governs the conduct of consensual wire, electronic, and oral interceptions for law enforcement purposes.

36-17.4. Using Network Security Monitoring Systems: When Does An "Interception" Take Place?

a. DoD, and Navy in particular, use network anti-intrusion security monitoring systems and software to automatically detect and capture electronic intrusions. Typically, such systems capture all activity on the network meeting criteria indicative of possible intrusion or unauthorized use; for example, capturing all attempts to exploit a known security weakness within the system, capturing all attempted introductions of "sniffer" programs, or capturing activity from particular accounts known to be used by "hackers", etc. Such network security systems will capture a great deal of activity in the blind that is of no interest to the system administrator or law enforcement official. Such captured material must be further screened to identify that activity that actually merits downloading and reading for content. After the screened material is downloaded and read for content, instances of actual and attempted intrusion can be identified and preserved as evidence.

b. As noted above, system administrators are authorized under the law to use network security monitoring systems. It is important to note that NCIS special agents can also utilize such monitoring systems in the course of law enforcement investigations. However, when a NCIS special agent utilizes a monitoring system specifically for law enforcement purposes, an issue arises concerning whether the special agent is consensually intercepting electronic communications. It is the opinion of Code 00L that a consensual interception occurs at the point at which the post-screened material is downloaded to permit reading for content. If a special agent has a need to intercept a particular criminal suspect's communications on the system, authorization for the intercept must be obtained in accordance with Section 36-4.

36-17.5. Gaining Access to Stored Electronic Communications.

a. The provider of an electronic communication service to the public (for example, America Online (AOL)) is prohibited from disclosing the contents of a communication held in electronic storage, unless he or she is authorized to do so by court order, or the originator, addressee, intended recipient, or subscriber consents, or the SYSOP inadvertently reads the communication and it appears to pertain to a crime. Similarly, the provider of a remote computing service to the public is prohibited from disclosing the contents of a communication carried or maintained on the service. In the latter case, the SYSOP may disclose the communication to a law enforcement agency.

b. The limitation on accessing stored electronic communications affects access to e-mail while it is being stored in a file server. Typically, e-mail is sent by an originator through a file server, where it is temporarily stored until it is retrieved by the addressee. While the e-mail is temporarily stored in the file server, it may not be obtained and read, unless one of the statutes exceptions apply.

c. There are three aspects of this law that should be noted:

(1) First, the originator, addressee, intended recipient, or subscriber may consent to the disclosure of the stored communication (e-mail).

(2) Second, the prohibition applies only to communication services and remote computing services provided to the public. A private computer system, for example a closed DoD system or a private employer's LAN, is not covered. Thus, e-mails sent between parties in a closed DoD system is not protected by this statute.

(3) In addition, a closed system does not change its status, and become a system "provided to the public" simply because it contains a modem pool or gateway file server that permits users to access public systems. For example, a DoD system that is not provided to the public, does not become a system "open to the public" simply because an authorized user can access the Internet through a modem pool or members of the public can access the DoD system.

36-17.6. The Privacy Protection Act (PPA) Title 42 USC Section 2000aa.

a. The Privacy Protection Act (PPA) was enacted in 1980 to afford the press and certain other persons not suspected of committing a crime with protections not provided currently by the Fourth Amendment. Its objective is to give some protection from government search and seizure efforts to persons involved in First Amendment activities who are not themselves suspected of participation in the criminal activity for which the materials are sought.

b. The PPA does not restrict the use of subpoenas, or court orders, or other legal process for surrender of evidentiary documents to government authorities even if intended for publication. In fact, the PPA favors the use of those less intrusive means. Concomitantly, the PPA does not diminish the basis for opposing such legal process, such as the "work product" defense to a subpoena. The PPA addresses search and seizure only.

c. Since 1980, the extensive and ever-increasing use of personal computers for publishing on the

World Wide Web (www) has increased the likelihood that individuals who are not suspected of a crime will be involved in First Amendment activities that process or contain information of importance to law enforcement. There are two important aspects of the PPA that bear emphasis. First, no federal officer or employee shall apply for a warrant to search for and seize documentary materials believed to be in the private possession of a disinterested third party unless the application for the warrant has been authorized by an attorney for the government. Second, there are civil liabilities for government agencies and individual federal officers and employees who violate the PPA.

d. The DOJ Computer Crime and Intellectual Property Section, at telephone (202) 514-1026, is the contact point for authorization to seek a search warrant for material implicating the PPA in computer searches. For all other searches implicating the PPA, the DOJ point of contact is the OEO Chief of Office, telephone (b)(6) Depending on the status of the disinterested third party holding the documentary materials (lawyer, clergy, physician, news organization, and others), the authorization decision might be made no lower than the Deputy Assistant Attorney General level.

APPENDIX (1): DEFINITIONS

Abroad. Outside the U.S., its territories and possessions. An interception takes place aboard when the interception device is located and operated outside the U.S. and the target of the interception is located outside the U.S.

Additional Target. An individual identified during the course of an investigation/operation as a target and for whom interception authority is being requested subsequent to the original authorization.

Consensual Interception. An interception by a person acting under color of law of a wire, oral, or electronic communication where such party to the communication or one of the parties to the communication has given prior consent to such interception (subsection 2511(2)(c) of Title18 USC).

Contents. When used about any wire, oral, or electronic communication includes any information on the substance, purport, or meaning of that communication (subsection 2510(8) of Title 18 USC).

Defense Criminal Investigative Organizations (DCIOs). Includes the U.S. Army Criminal Investigation Command (USACID), the Naval Criminal Investigative Service (NCIS), the Air Force Office of Special Investigations (AFOSI), and the Defense Criminal Investigative Service (DCIS).

DoD Personnel. Civilian employees of the Department of Defense, active and Reserve duty members of the Military Services, retired members of the Military Services, and dependents of civilian employees and active duty members.

Electronic Communication. Any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic or photo-optical system that affects interstate or foreign commerce, but does not include:

a. Any wire or oral communication; or,

b. Any communication made through a tone-only paging device; or

c. Any communication from a tracking device (as defined in Section 3117 of Title 18 USC), or,

d. Electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds.

Electronic Communication Service. Any service that provides to users thereof the ability to send or receive wire or electronic communications (subsection 2510(15) of Title 18 USC).

Electronic Communications System. Any wire, radio, electromagnetic, photo optical or photo electronic facility for the transmission of electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.

Electronic Storage.

a. Any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

b. Any storage of such communication by an electronic communication service by backup protection of such communication (subsection 2510(17) of Title 18 USC)

Inadvertent Interception. The unanticipated oral/wire interception of a conversation between a consenting party and an individual not previously identified as a target and for whom interception authority has not been granted.

Interception. The aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical or other device.

Oral Communication. Any oral communication uttered by a person exhibiting an expectation that such communication is not subject to interception, under circumstances justifying such expectation. But such term does not include any electronic communication.

Pen Register. A device which records or decodes electronic or other impulses which identify the numbers dialed or otherwise transmitted on the telephone line to which such device is attached, but such term does not include any device used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communications services provided by such provider or any device used by a provider or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of its business.

Public Official. An official of any public entity of the Government, including special districts, Federal, State, county, and municipal governmental units.

Remote Computing Service. The provision to the public of computer storage or processing services by means of an electronic communications system (subsection 2711(2) of 18 USC).

Tracking Device. The term "tracking device" means an electronic or mechanical device that permits the tracking of the movement of a person or object.

Trap and Trace. A device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or electronic communication was transmitted.

Unauthorized Interception. The willful oral/wire interception of a conversation between a consenting party and an individual for whom authority has not been granted.

United States. The 50 states of the U.S., the District of Columbia, the Commonwealth of Puerto Rico, and any territory of possession of the U.S.

a. The term "United States person" means:

(1) A United States citizen;

(2) An alien known by the DoD intelligence component concerned to be a permanent resident alien;

(3) An unincorporated association substantially composed of U.S. citizens or permanent resident aliens;

(4) A corporation incorporated in the U.S., except for a corporation directed and controlled by a foreign government or governments. A corporation or corporate subsidiary incorporated abroad, even if partially or wholly owned by a corporation incorporated in the U.S., is not a United States person.

b. A person or organization outside the U.S. shall be presumed not to be a United States person unless specific information to the contrary is obtained. An alien in the U.S. shall be presumed not to be a United States person unless specific information to the contrary is obtained.

User. Any person or entity who:

a. Uses an electronic communication service; and

b. Is duly authorized by the provider of such service to engage in such use.

Wire Communications. Any aural transfer made in whole or part though the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce and such term includes any electronic storage of such communication.

APPENDIX (2): CONSENSUAL INTERCEPT WAIVER

US NAVAL CRIMINAL INVESTIGATIVE SERVICE
CONSENSUAL INTERCEPT WAIVER

Date:

Location:

I,_____, authorize special agents of the Naval Criminal Investigative Service to place a body recorder and/or transmitter on my person and/or a recording device on a telephone located at _____for the purpose of recording any conversation I may have with _____ during the period _____ . I voluntarily give this written permission. No threats or promises have been extended to me.

_____
Signature

_____
Witnessed by:

APPENDIX (3): RECORDING OF INTERROGATIONS

The following are factors for consideration by Special Agents-in-Charge or their designees when determining whether to record interrogations. These factors are neither inclusive nor restrictive and are not regulating guidelines. They should not be viewed as a checklist and are not intended to limit supervisory decision-making. They are intended to be thought provoking to assist in the decision making process when considering whether to record an interrogation and are consistent with factors considered by other federal law enforcement agencies:

1. Recording interrogations in non-violent crimes shall be strongly considered in those cases that lack evidence the person being interviewed committed the offense.

2. Whether the purpose of the interrogation is to gather evidence for prosecution, or intelligence for analysis, or both.

3. If prosecution is anticipated, the type and seriousness of the crime, including, in particular, whether the crime has a mental element (e.g., knowledge or intent to defraud), proof of which would be considerably aided by the subject's admission own words.

4. Whether the subject's own words and appearance (in video recordings) would help rebut any doubt about the voluntariness of the statement raised by a person's age, mental state, educational level or understanding of the English language; or is otherwise expected to be an issue at trial, such as to rebut an insanity defense; or perhaps be of value to behavioral analysts.

5. The preference of the Military Trial Counsel, the U. S. Attorney's Office (USAO) or Federal District Court regarding recorded statements.

6. Local laws and practice - particularly in task force investigations where state prosecution is possible.

7. Whether interrogations with other subjects in the same or related cases have been electronically recorded.

8. The potential to use the subject as a cooperating witness and the value of using his/her own words to elicit his/her cooperation.

9. Practical considerations - such as the expected length of the interrogation; the availability of recording equipment and transcription (and if necessary, translation) services; and the time and available resources required to obtain them.

APPENDIX (4): SAMPLE BANNERS

Telephone

DO NOT DISCUSS CLASSIFIED INFORMATION
This telephone is subject to monitoring at all times. Use of this telephone constitutes consent to monitoring

DD FORM 2056, MAY 2000 Previous editions may be used.

Computer

STANDARD MANDATORY
DOD NOTICE AND CONSENT BANNER

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

- At any time, the USG may inspect and seize data stored on this IS.

- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

- Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

Pages 1116 through 1123 redacted for the following reasons:
- -
(b)(6), (b)(7)(C), (b)(7)(E)
(b)(7)(E)

NCIS-3, CHAPTER 37
BIOMETRICS
EFFECTIVE DATE: JANUARY 2014

Table of Contents

References:

(a) DoD Instruction 5505.11/ 9 Jul 2010/Fingerprint Card and Final Disposition Report Submission Requirements (incorporating Change 1/3 May 2011)
(b) Public Law 106-523 Military Extraterritorial Jurisdiction Act of 2000 of 22 Nov 2000; Chapter 212, Sections 3261–3267, of title 18, United States Code Personnel Subject to Uniform Code
(c)) Deputy Secretary of Defense Memorandum, "Responsibility for Response to Reports of Alleged Criminal Activity Involving Contractors and Civilians Serving with or Accompanying the Armed Forces Overseas," September 10, 2008
(d) DoD 8910.1-M/30 June 1998/Department of Defense Procedures for Management of Information Requirements
(e) U.S. Supreme Court, Middendorf v. Henry, 425 U.S. 25 (1976)
(f) Privacy Act of 1974, 5 U.S.C. 552a (2000)
(g) SECNAVINST 5211.5E/28 Dec 2005/Department of the Navy Privacy Program
(h) NCIS-1, Chapter 21 Personal Privacy and Rights of Individuals (Privacy Act)
(i) Criminal Justice Information Services (CJIS)/13 Jul 2012/ Security Policy Version 5.1.
(j) DoD Directive 8521.01E/21 Feb 2008/Department of Defense Biometrics
(k) DoD 5240.1-R/07DEC82/Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons
(l) Immigration and Nationality Act of 1952, 66 Stat. 233, 8 U.S.C. § 1357(a)

37-1. Purpose. This chapter documents policy and procedures for collecting biometric and associated (biographic and situational) information on subjects for a variety of purposes and settings. This chapter details how NCIS personnel can submit this information to authoritative U.S. Government (USG) identity systems to promote the success of their missions. The USG identity systems that primarily support NCIS are the Federal Bureau of Investigation (FBI) Criminal Justice Information Service Division (CJIS) Integrated Automated Fingerprint Identification System (IAFIS), the Department of Defense (DoD) Automated Biometric Identification System (ABIS), and the Department of Homeland Security (DHS) automated biometric identification system (IDENT).

37-2. Policy. This chapter establishes the policy for responsibilities, requirements, and standards for the collection and use of biometric data to support NCIS missions and objectives. Information contained in this chapter is based on the higher authorities cited in this text. The provisions of this chapter apply to all NCIS personnel that leverage biometric technology or data.

37-3. Cancellation. This chapter cancels NCIS-1, Chapter 25.1 section 19 and NCIS-3, Chapter 6 section 19.

37-4. Chapter Sponsor. The chapter sponsor is the Biometrics Division, Code 25A.

37-5. Introduction

a. Biometrics is a general term employed to describe a physical characteristic or a process used to establish the positive identity of an individual. As a characteristic, biometrics is the measure of a biological (anatomical and physiological) or behavioral feature that can be used for automated recognition. At present, NCIS and the USG mainly use three biometrics operationally: face, fingerprint, and iris images. As a process, biometrics is a method of automated recognition of an individual by measurable biological (anatomical and physiological) and behavioral characteristics.

b. Positive identification is critical to investigative and operational processes, and in the proper handling of suspects, persons of interest, and sources. Criminals, terrorists, and spies can alter or fabricate names, uniforms, addresses, identification papers, social security cards, and other forms of presumptive identification, but they cannot change their biometric characteristics. NCIS' use of biometric collection devices increases the speed and effectiveness of identifying subjects and gaining additional information on those already identified.

c. NCIS participates in a broad interagency enterprise to leverage biometrics and develop identity intelligence. The primary USG biometric data storage and search systems are IAFIS, ABIS, and IDENT. (b)(7)(E)

(b)(7)(E)

ABIS identity records may contain face, fingerprint, and iris images as well as latent fingerprints from terrorist and other criminal incidents. IDENT is composed of the identity records collected from visa applications, border crossings, and DHS law enforcement activities such as interdicting illegal entry to the U.S. IDENT contains face and fingerprint images.

d. NCIS provides support for criminal investigative, force protection, and counterintelligence missions through the use of biometric collection devices. At present, NCIS deploys Cross Match Live Scan and Cross Match Secure Electronic Enrollment Kit (SEEK) devices. This chapter refers to devices as either Live Scans, in the case of stationary devices used to collect fingerprints to support law enforcement activities, or as SEEKs when referring to mobile handheld devices that support a wider range of activities. As the biometric marketplace evolves, NCIS may use other devices in place of the current suite of tools and will update this chapter to reflect any such changes.

e. Live Scan fingerprint collection devices enable investigative personnel to collect or query fingerprints for criminal investigations. SEEK devices enable users to collect or query face, fingerprint, or iris images for a range of missions. NCIS provides biometric enabled intelligence (BEI) analysis support that can be initiated by these biometric collections and queries.

f. NCIS investigative personnel can collect and submit biometric (face, fingerprint, and iris images) and other supporting information (including biographic or contextual) to enroll or query USG systems such as ABIS, IAFIS, and IDENT. When NCIS enrolls biometrics, USG systems search their holdings and create or update permanent records. NCIS queries search systems without creating or updating records. For both, any information discovered is returned to users via the submitting Live Scan or, for SEEK submissions, via a Web portal and/or e-mail.

g. While supporting criminal investigations, NCIS collects and submits all fingerprints and associated information via Federal Document 249 (FD-249) "Suspect Fingerprint Card." This can be done electronically via a Live Scan or via a paper FD-249, if a Live Scan is not available.

(1) Live Scan fingerprint collection devices. NCIS uses Live Scan devices to collect face and fingerprint images, and associated information. A Live Scan device compiles this data in an electronic FD-249, and transmits the FD-249 to IAFIS for enrollment or query. For criminal enrollments, this record is linked to the Interstate Identification Index (III or "Triple I") which will provide any Criminal History Record Information (CHRI) in the form of a Report of Arrest and Prosecution (RAP Sheet).

(2) Paper FD-249s (Fingerprint Cards). NCIS uses paper FD-249 cards for IAFIS enrollments only when a Live Scan device is not available. If a Live Scan device is available, fingerprints and associated information shall be collected using the Live Scan device. Although the FBI no longer directly accepts paper FD-249s, the Biometrics Division will continue to scan paper FD-249s and submit them electronically, when required. The

(b)(7)(E)

h. NCIS collects and submits biometric and other information via SEEKs for non-criminal investigation use. SEEK devices enable users to collect face, fingerprint, and iris images, as well as associated information through the devices' sensors and keypad. This information is compiled into a digital file which is transmitted to ABIS for enrollment or query. Depending on the mission, users will transmit data either through a Web portal or via e-mail. Users should contact the Biometrics Division (Code 25A4) for assistance in configuring SEEK transmissions.

i. Submission Results. Every submission to an identity system, whether an enrollment or query, will result in either a "match" or "no match" response. "Match" responses occur when the subject being searched has previously been enrolled in the target identity system. Otherwise, systems return a "no match" response. Matches do not necessarily indicate that a subject is a threat, as USG identity systems contain information on travelers and third party nationals that have been cleared to work on U.S. military installations. When the subject has been placed on a system's watchlist of known or suspected threats, the resultant match will be cited as an "alert" indicating that there is derogatory reporting on the subject.

j. The NCIS Biometrics Division can be reached via e-mail at (b)(6), (b)(7)(C) @NCIS.Navy.mil.

37-6. Collecting and Submitting Criminal Fingerprints

a. NCIS investigative personnel shall submit fingerprints and associated information to IAFIS to initiate or update a subject's Criminal History Record Information (CHRI) upon the establishment of probable cause that a U.S. military member has committed offenses listed in reference (a) or a civilian has committed offenses equivalent to those listed in reference (a). This applies to the following:

(1) Members of the Military Services investigated for offenses listed in reference (a) by defense criminal investigative organizations (DCIOs) or other DoD law enforcement organizations.

(2) Civilians investigated for offenses equivalent to those listed in reference (a). This includes foreign nationals, persons serving with or accompanying Armed Forces in the field in time of declared war or contingency operations, and persons subject to reference (b) in accordance with reference (c).

(3) Military Service members, their dependents, and DoD employees and contractors investigated by foreign law enforcement organizations for offenses equivalent to those listed in enclosure (2) to reference (a), and made available to the DCIOs or other DoD law enforcement organizations.

b. NCIS shall initiate or update a subject's CHRI by collecting fingerprints and associated information via an FD-249 via a Live Scan device, when available, or on a paper FD-249 when a Live Scan device is not available. NCIS personnel shall submit FD-249s to IAFIS either by transmitting through the Live Scan device or by mailing the paper FD-249 to NCIS HQ. The submission shall occur within 15 days of establishing probable cause but not earlier than apprehension (U.S. military member), arrest (civilian) or subject interview. The following procedures apply:

(1) For U.S. military subjects investigated by NCIS, the FD-249 shall be submitted within 15 days of determining that probable cause exists to believe that the subject has committed an offense listed in reference (a).

(2) For civilian suspects investigated by NCIS, the FD-249 shall be submitted within 15 days of the interview, arrest, or indictment, as applicable, for offenses punishable pursuant to the United States Code (U.S.C.) that are equivalent to those listed in reference (a).

c. Fingerprints shall not be held pending a command decision, final adjudication, or appellate action. Reference (a) explicitly forbids the practice of delaying the submission for any reason including the expectation that final disposition will be available within 60 days.

d. The following data shall be recorded on the FD-249:

(1) Fingerprints:

(a) Ten fingerprint images individually taken by rolling from nail to nail.

(b) Two flat impressions of the thumbs (right and left).

(c) Two flat impressions of the four fingers (taken together) on the left hand and on the right hand.

(2) Associated information:

(a) Biographic:

1. Block 1: Name (NAM)

2. Block 3: Social Security number (SSN) (if known), or 000-00-0000 if the SSN is not known

3. Block 7: Place of birth (POB)

4. Block 8: Gender (SEX)

5. Block 9: Race (RAC)

6. Block 10: Height (HGT)

7. Block 11: Weight (WGT)

8. Block 12: Eye color (EYE)

9. Block 13: Hair (HAI)

10. Block 20: Place of Birth (POB)

11. Block 21: Citizenship (CTZ)

12. Block 23: Scars/Marks/Tattoos (SMT)

13. Block 24: Residence/Complete Address (ADR)

14. Block 28: Occupation (if known)

15. Block 29: Employer or Command (if known)

(b) Situational:

1. Block 16: Date of Arrest (DOA)

2. Block 19: Date of Offense (DOO)

3. Block 25: Official Taking the Fingerprint

4. Block 27: Check boxes to indicate whether "Photo available?" and/or "Palm prints taken?"

5. Block 30: Charges/Citations

6. Block 31: Disposition (if available)

(c) Charges:

1. Investigative personnel shall ensure that the charges annotated on the FD-249 reflect the actual charges being pursued through courts-martial or nonjudicial punishment, or the anticipated charges based upon the established probable cause.

2. For U.S. military members, the FD-249 shall include the Uniform Code of Military Justice (UCMJ) Article, U.S.C. section, state or other citation, and the charges shall be written out in plain language (e.g., UCMJ Article121-Larceny, UCMJ Article 128-Assault). Offenses shall not be described solely by references to a UCMJ punitive article or to the U.S.C. or other statutory provision.

3. For civilians, the FD-249 shall include the specific U.S.C. section, state or other citation and the charges, which shall be listed in commonly understood and descriptive terms such as robbery and larceny as required by the FBI.

e. In the Report of Investigation (ROI) (INTERIM), NCIS Code 25A4 shall be listed in the ACTION line, with no response required to this tasking. For Live Scan FD-249 submissions, the transaction control number shall be listed in the ACTION line. For paper FD-249 submissions, the certified mail number shall be listed in the ACTION line. For all FD249s (Live Scan or paper) the number of face images submitted shall also be included in the ACTION line.

f. Reporting final disposition. If final disposition is available within 15 days of determining probable cause, it may be reported on the FD-249 in lieu of the FBI form R-84, entitled Final Disposition Report.

g. Submitting paper FD-249s. Paper FD-249s shall be used only when a Live Scan is not available. All FD-249s will be reviewed for quality conformance with CJIS enrollment standards and will be returned if the fingerprints do not meet these standards or if the associated information is missing or incomplete. Paper FD-249s shall be submitted as follows:

(1) Send two separate paper FD-249s to NCISHQ. Retention of a copy of the FD-249 in the case file is recommended in the uncommon case that the two paper FD-249s do not reach their destination.

(2) The FD-249s with face image photographs shall be submitted by certified mail or a delivery service that ensures tracking information equivalent to certified mail. The FD-249s shall be sent to:

Naval Criminal Investigative Service
Russell-Knox Building
ATTN: Code 25A4 (FINGERPRINTS)
27130 Telegraph Road
Quantico, VA 22134

(3) FD-249s shall be the current FBI version employed by NCIS and shall not be procured from other agencies as these may include information, markings, or formatting specific to that agency.

(4) It is the responsibility of the submitter to ensure that all required information, including the name of the person who collected the fingerprints, is entered on the FD-249. The enrollment of an FD-249 without the proper identification information may be delayed or returned to the submitting office for correction and resubmission.

(5) Submitting NCIS components shall maintain a reserve of FD-249 paper cards. NCIS components shall request paper FD-249s from the Biometrics Division as needed to ensure this reserve.

(6) An FD-258 "Applicant" card for criminal background checks prior to employment may not be used in place of the FD-249.

h. Submitting FD-249s by scanning. A completed FD-249 may be scanned and e-mailed with face image photographs attached (for digital photograph requirements, please see section 37-11d(3)). The FD-249 shall be scanned on an IAFIS Certified Product List (CPL) scanner at a resolution of at least 500 pixels per inch (ppi), though 1,000 ppi is preferred provided the resultant file size does not exceed transmission size limitations. The scanned FD-249 shall be saved and e-mailed in JPEG or JPEG 2000 format set not to exceed a 10:1 compression ratio. The electronic FD-249 shall be e-mailed to the Biometrics Division in an encrypted e-mail. The submitter shall contact the Biometrics Division to identify an e-mail address to e-mail the encrypted FD-249. All scanned FD-249s will be reviewed for quality conformance with CJIS enrollment standards and will be returned if the fingerprints do not meet these standards or if the associated information is missing or incomplete. Prior coordination with the NCIS Biometrics Division is required to inform the biometric analyst of the submission and to establish a point of contact to report results.

i. Consolidated Law Enforcement Operations Center (CLEOC) Reporting. All enrollments into IAFIS as well as the reporting of final disposition shall be documented in the ROI and noted in CLEOC. Reference (d) exempts DoD internal reporting of CHRI data from review and approval.

37-7. Reporting Final Dispositions

a. For each fingerprint file enrolled in IAFIS via FD-249, the submitting component shall report the final disposition information. Final disposition may be reported on the FD-249 if this is known before the 15-day enrollment deadline. If determined after the submission of the FD-249, final disposition shall be reported on an R-84.

b. Do not hold the R-84 pending appellate actions. Appellate action affecting the initial disposition shall be reported, if it occurs, using an additional R-84 to update the CHRI.

c. Military. For military proceedings, submit an R-84 within 15 calendar days after final disposition of military judicial or nonjudicial punishment, or the approval of a request for discharge, retirement, or resignation in lieu of court-martial.

(1) Courts-martial. For courts-martial, specify whether it was a general, special or summary court-martial. Include the following:

(a) The date of punishment or dismissal.

(b) The charges. Charges shall be written in commonly understood descriptive terms (e.g., murder, rape, robbery, assault, possession of a controlled substance) or by a commonly understood title. The charges on the R-84 should reflect those on the submitted FD-249.

(c) The UCMJ article, the U.S.C. section, the state or other citation or statute for each charge as reported on the FD-249. Offenses shall not be described solely by references to a UCMJ punitive article, the U.S.C. section or other statutory provision.

(d) The offenses for which the individual was convicted, acquitted, or whether the charges were dismissed or withdrawn.

(e) The sentence or punishment awarded by a court-martial such as confinement, punitive action, reduction in pay grade, fines, forfeitures of pay, or discharge (and type of discharge).

(f) Adverse findings resulting from a summary court-martial should be recorded as follows: "Subject found guilty by summary court-martial." Although action by a summary court-martial is disciplinary in nature for a violation of military law, a summary court-martial is not a criminal proceeding per reference (e). The disposition of "conviction" shall only be reported for crimes prosecuted by general or special court-martial resulting in a finding of guilty.

(2) Nonjudicial punishment. For the outcome of military nonjudicial punishment include the following:

(a) Nonjudicial punishment pursuant to Article 15 of the UCMJ shall be recorded as "nonjudicial disciplinary action." Punishment pursuant to Article 15 of the UCMJ is a disciplinary action, but does not constitute a criminal proceeding or conviction and should not be recorded as such.

(b) The UCMJ article, the USC, state, or other citation or statute for each charge as reported on the FD-249.

(c) The outcome of the adjudication or the nonjudicial punishment described in common language (such as punitive discharge and type of discharge, confinement, reduction in rank, forfeiture of pay or charges dismissed). A sentence of no punishment should be listed as "no punishment."

(d) The date of the nonjudicial punishment or the date of approval of the request for retirement or resignation.

(e) The offenses for which the individual was punished or that were the basis for the retirement or resignation.

d. Civilian. For civilian proceedings, submit R-84 within 15 calendar days after final disposition and include the following:

(1) The date of adjudication and the adjudicative forum.

(2) The U.S.C. violation, state, or other citation, or statute as appropriate with a description of each offense as reported on the FD-249.

(3) The disposition of each charge such as convicted, acquitted, withdrawn, dismissed or not prosecuted.

(4) The sentence, if convicted.

e. Dispositions that are exculpatory in nature (e.g., dismissal of charges or acquittal) shall also be documented using the R-84.

f. The FBI number shall be entered at the top left corner of the R-84 to match the final disposition with existing CHRI.

g. The submitting component is responsible for sending the R-84 directly to the FBI. Although not required, preaddressed stamped envelopes for this purpose are available through the Biometrics Division. FBI's CJIS Division address:

Federal Bureau of Investigation
Criminal Justice Information Services Division
Clarksburg, WV 26306

h. A reserve of R-84s shall be kept on hand at each NCIS component. Additional R-84s shall be obtained by contacting the NCIS Biometrics Division.

i. NCIS Internal Reporting. The reporting of final disposition shall be documented in the ROI. Reference (d) exempts DoD internal reporting of CHRI data from review and approval. The last paragraph of the ROI (CLOSED) should reflect the date final disposition was mailed to the FBI. (Example: on DDMMMYYYY, S/Doe's Final Disposition Report was mailed to the FBI Criminal Justice Information Services Division, Clarksburg, WV. This investigation is closed.)

37-8. Querying Fingerprints from Persons of Interest, Victims, Witnesses, and Sources in Support of Criminal Investigations via Live Scan

(b)(7)(E)

Pages 1134 through 1142 redacted for the following reasons:
- -
(b)(7)(E)

(b)(7)(E)

37-15. Acronyms

a.	ABIS	Automated Biometric Identification System
b.	BEI	Biometrics Enabled Intelligence
c.	BEWL	Biometrics Enabled Watchlist
d.	CHRI	Criminal History Record Information
e.	CJIS	Criminal Justice Information Services Division
f.	CPL	Certified Products List
g.	DCIO	Defense Criminal Investigative Organization
h.	DFBA	Defense Forensics and Biometrics Agency (formerly Biometrics and Identity Management Agency [BIMA])
i.	DoD	Department of Defense
j.	DPAS	Defense Property Accountability System
k.	EBTS	Electronic Biometrics Transmission Specification
l.	EMIO	Expanded Maritime Interception Operation
m.	FBI	Federal Bureau of Investigation
n.	IAFIS	Integrated Automated Fingerprint Identification System
o.	IDENT	DHS Automated Biometric IDENTification System
p.	III	Interstate Identification Index
q.	MIO	Maritime Interception Operation
r.	MTAC	Multiple Threat Alert Center
s.	NCIC	National CrimE Information Center
t.	PII	Personally Identifiable Information
u.	RAP	Record of Arrest and Prosecution
v.	ROI	Report of Investigation

w.	SSD	Standard System Document
x.	UCMJ	Uniform Code of Military Justice
y.	USC	United States Code

37-16. Key Terminology

a. Associated information (also known as contextual data). The 1) biographic (such as name, height, date of birth) and 2) situational information (such as the reason for arrest, circumstance of collecting the biometrics, warnings) about a person collected with the biometric samples.

b. Automated Biometric Identification System (ABIS). The DoD ABIS is an electronic database and an associated set of software applications that support the storage, retrieval, and searching of biometric and associated information collected from persons of national security interest.

c. Biometric characteristic. A biological and/or behavioral characteristic of an individual that can be detected and from which distinguishing, repeatable biometric features can be extracted for the purpose of automated recognition.

d. Biometric-Enabled Intelligence (BEI). The intelligence resulting from the collection, processing, analysis and interpretation of biometric signatures; the contextual data associated with those signatures; and other available intelligence concerning persons, networks or populations of interest.

(1) BEI as a product. The intelligence resulting from the collection, processing, analysis and interpretation of the biometrics and the associated information with the biometrics and other available intelligence.

(2) BEI as a process. A specialized analytical discipline that relies on all-source collections and a distinct processing, exploitation, reporting and dissemination enterprise to integrate information derived from biometric collection and processing into all-source intelligence analysis.

e. Biometrics Enabled Watchlist (BEWL). A list of persons of interest, whose subjects can be identified through biometric signatures. Such lists may include other information, such as names and the desired/recommended disposition instructions for each individual. The DoD produces a BEWL which can be loaded to SEEKs for mobile matching.

f. Biometric file. The standardized individual data set resulting from a collection and composed of the biometric sample(s) and associated data (biographic data and situational information.)

g. Biographic information. Data that describes physical and non-physical attributes of a biometric subject from whom biometric sample data has been collected. For example, full name, age, height, weight, address, employers, telephone number, e-mail address, birthplace,

nationality, education level, group affiliations, employer, security clearances, financial and credit history. (Biographic plus situational information constitutes associated information accompanying a biometric sample. See associated information.)

h. Biometric record. A data record containing biometric and associated information against which a submission is searched.

i. Biometric sample. The physical biometrics collected (face, fingerprint, and iris images).

j. Biometrics. A general term used alternatively to describe a characteristic or a process.

(1) As a characteristic. The measure of a biological (anatomical and physiological) and/or behavioral biometric characteristic that can be used for automated recognition.

(2) As a process. Automated methods of recognizing an individual based on the measure of biological (anatomical and physiological) and/or behavioral biometric characteristics.

k. Collection. Capturing biometric sample(s) and associated data from a biometric subject, with or without his or her knowledge.

l. Criminal History Record Information (CHRI). Information on individuals collected by criminal justice agencies that consists of identifiable descriptions and notations of arrests, detentions, indictments, information or other formal criminal charges and any disposition arising from these, including acquittal, sentencing, correctional supervision and release. The term does not include investigative information, including medical and psychological treatment information or additional identification information not related to an individual's involvement with the criminal justice system.

m. Criminal Justice Information Services (CJIS) Division. The FBI's CJIS Division was established to serve as the focal point and central repository for criminal justice information services in the FBI. CJIS administers IAFIS, the National Crime Information Center (NCIC), (including files of interest to law enforcement, such as those relating to wanted persons, civil protection orders, registered sex offenders, and missing persons), the national Interstate Identification Index (III) criminal history record index, and the National Instant Criminal Background Check System (NICS).

n. Electronic Biometrics Transmission Specification (EBTS). Standards-based format used to facilitate the collection of biometrics and enhance interoperability with IAFIS, ABIS and other biometric systems.

o. Enrollment (Search/ Retain Data). Submitting biometric and associated information to create or update a record on an individual. These data will be permanently stored. Any match information is returned to the submitter.

p. Fingerprint File. The collected fingerprint images, associated biographic and situational (related to the circumstances, such as a criminal apprehension, under which the fingerprints

were collected) information and face image photographs. NCIS investigative personnel will submit fingerprint files to IAFIS for the purposes of an enrollment or a query.

q. IAFIS Certified Products List (CPL). Provides users with a list of products that have been tested and are in compliance with IAFIS Image Quality Specifications (IQS) regarding the capture of friction ridge images. Specifications and standards other than image quality may still need to be met. A list of FBI certified products may be found at: https://www.fbibiospecs.org/IAFIS/Default.aspx

r. IDENT. IDENT is the DHS-wide system for the storage and processing of biometric and limited biographic information for national security, law enforcement, immigration, intelligence and other DHS mission-related functions.

s. Identity Record. The information stored on an individual within an identity system. Identity records may store biometric data along with other associated data, such as biographical or situational information. Biometrically-enabled systems such as ABIS, IAFIS, and IDENT enable searching against biometric data associated with subjects.

t. Integrated Automated Fingerprint Identification System (IAFIS). The FBI's large-scale ten fingerprint (open-set) identification system is used for searches for CHRI and the identification of latent prints discovered at crime scenes. This system provides automated and latent search capabilities, electronic image storage, and electronic exchange of fingerprints and responses.

u. Match. Based on an automated comparison, a biometric sample submitted to an authoritative database and an existing identity or criminal biometric record are from the same source.

v. Modality. A type or class of biometric sample originating from a biometric subject such as face, fingerprint or iris image. Additional modalities include hand geometry, palm print, voice print, gait, keystroke dynamics, signature dynamics among others.

w. Personally Identifiable Information (PII). Information that can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, and biometric records, including any other personal information which is linked or linkable to a specific individual.

x. Probable Cause. Probable Cause is determined as a result of facts and circumstances, more than mere suspicion but less than proof beyond a reasonable doubt, that would lead a reasonable and prudent person to believe that a crime has been, is being, or is about to be committed, and that the individual in question has committed the crime.

y. Query (Search/Do Not Retain Data). Submitting biometric and associated information to search a biometric data system without retaining the biometric file or creating or updating biometric record. Any match information is returned to the submitter.

z. Screening. The physical process of reviewing a person's presented biometric and associated information to determine their authenticity, authorization, and credential verification against a government data source through authorized and secure channels at any-time during the person's period of physical access eligibility. This assessment identifies derogatory actions that can be determined as disqualifying issues for current or continuing physical access eligibility standards and requirements for the resource, asset, or installation.

aa. Situational information. The "who, what, when, where, how, why," etc. associated with a collection event and permanently recorded as an integral component of associated information. (Biographic plus situational information constitutes associated information accompanying a biometric sample. See associated information.)

ab. Submission. The act of sending the biometric file to IAFIS or ABIS for enrollment or querying.

ac. U.S. Person. A U.S. citizen or an alien who is a legal permanent resident alien.

ad. Vetting. An evaluation of an applicant's or a card holder's character and conduct for approval, acceptance or denial for the issuance of an access control credential or physical access.

NCIS-3, Chapter 38
Force Protection Activities
Effective Date: APRIL 2015

TABLE OF CONTENTS **PAGE**

38-1. Purpose. This chapter provides guidance on carrying out the responsibility of the Naval Criminal Investigative Service (NCIS) to provide force protection (FP) support to the Department of the Navy (DON) and the Department of Defense (DoD). NCIS provides comprehensive, aggressive, and integrated counterintelligence (CI) capabilities throughout the DON, using all CI functions and related activities, to support the FP programs of DON and DoD Components and other supported elements.

38-2. Policy. NCIS field offices will provide full-spectrum CI support to FP throughout the DON to mitigate and prevent attacks in accordance with the authorities and provisions contained in reference (a). The policies and instructions from which NCIS derives its CI support to FP-related authorities are listed in Appendix A. A list of acronyms and abbreviations used throughout this chapter is found in Appendix B. For policy on the Country Referent Program policy, see Appendix C. For Force Protection Detachment (FPD) policy, see Appendix D. For Security Training Assistance and Assessment Teams (STAAT) policy, see Appendix E. For Port Visit Support (case category 5C) policy, see Appendix F. For Threat Assessment (case category 5G) policy, see Appendix G. For Force Protection Support (case category XXFP), see Appendix H. A sample XXFP ROI (INTERIM) is provided as Appendix I. For Exercise Participation (case category XXEX) policy, see Appendix J. A sample XXEX ROI (INTERIM) is provided as Appendix K. For Force Protection Activities (case category XXEV) policy, see Appendix L. A sample XXEV ROI (INTERIM) is provided as Appendix M.

38-3. Cancellation. The following policy issuances are canceled:

a. NCIS-3, Chapter 38, dated November 2008.

b. Gen Admin 21A-0007, NCIS Port Protection Tracker (5C) Database, dated March 16, 2010.

c. Gen Admin 21A-0020, NCIS Port Protection Tracker (5C) Database Enhancements, dated May 10, 2010.

d. Gen Admin 21A-0039, NCIS Port Protection Tracker (5C) Database Clarification of the types of Port Visit Support, dated August 13, 2010.

e. Gen Admin 22A-0010, National Security Directorate Program Guidance: Naval Criminal Investigative Service Participation in FPDs, dated February 28, 2012.

f. Gen Admin 11C-0028, NCIS Policy Document: 10-14 Operational (New NCIS Threat Assessment Protocol), dated October 14, 2012.

38-4. Chapter Sponsor. National Security Directorate, Code 22.

APPENDIX A
REFERENCES

(a) SECNAV Instruction 5430.107, Mission and Functions of the Naval Criminal Investigative Service, 28 December 2005

(b) DoD Instruction 5240.22, Counterintelligence Support to Force Protection, 24 September 2009, incorporating Change 1 dated October 15, 2013

(c) DoD Force Protection Detachment Joint Standard Operating Procedures (JSOP), revised September 2011

(d) NCIS-3, Chapter 8, Central Source Registry, 4 March 2011

(e) NCIS-8, STAAT Manual, November 2009

(f) NCIS-1, Chapter 2, Missions and Organization Structure

(g) OPNAV Instruction 5530.14E, Navy Physical Security and Law Enforcement Program, 28 January 2009, incorporating Change 2 effective December 8, 2006

(h) OPNAV Instruction F3300.53C, Navy Antiterrorism Program, 6 May 2009

(i) DoDI 2000.16, DoD Antiterrorism (AT) Standards, October 2, 2006, incorporating Change 2 dated December 8, 2006

(j) DoD Directive 5200.27, Acquisition of Information Concerning Persons and Organizations Not Affiliated with the Department of Defense, 7 January 1980

(k) DoD 5240.1-R, Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons, December 1982

(l) ICD 203, Analytic Standards, 21 June 2007

(m) ICD 206, Sourcing Requirements for Disseminated Analytic Products, 17 October 2007

(n) ICD 208, Write for Maximum Utility, 17 December 2008

(o) DoD Instruction 2000.12, DoD Antiterrorism (AT) Program, March 1, 2012, incorporating Change 1 dated September 9, 2013

(p) NCIS-4, NCIS Counterintelligence Manual, 7 July 2009

(q) DoD Instruction 5240.16, Counterintelligence Functional Services (CIFS), 27 August 2012, incorporating Change 1, Effective October 15, 2013

APPENDIX B
ACRONYMS AND ABBREVIATIONS

AFOSI	Air Force Office of Special Investigations
AOR	area of responsibility
AT	antiterrorism
CCICA	command counterintelligence coordinating authority
CCMD	combatant command
CCO	Counterintelligence and HUMINT Community Coordination Office
CIR	Criminal Intelligence Report
CLEOC	Consolidated Law Enforcement Operations Center
CM	collection manager
COM	chief of mission
CSO	chief staff officer
CSR	Central Source Registry
CT	counterterrorism
DATT	defense attaché
DIA	Defense Intelligence Agency
DOS	Department of State
FP	force protection
FPD	force protection detachment
HOTR	HUMINT Online Tasking and Reporting
ICD	Intelligence Community Directive
IOS	Intelligence operations specialists
IIR	intelligence information report
JSOP	joint standard operating procedures
LA	lead agency
LE	law enforcement
MDA	maritime domain awareness
MTAC	Multiple Threat Alert Center
NEO	noncombatant evacuation operations
NSF	Naval Security Forces
OFCO	offensive counterintelligence operation
PA	Port Assessment
PKO	peacekeeping operations
RFI	request for information
RSO	regional security officer
SDO	senior defense official
SIO	senior intelligence officer
SSIC	Security Specialist In Charge
STAAT	Security Training Assistance and Assessment Teams
TA	Threat Assessment
USG	U.S. Government
XXFP	Force Protection Support report

Pages 1152 through 1177 redacted for the following reasons:
- -
(b)(7)(E)

NCIS-3, CHAPTER 39
CRISIS MANAGEMENT
EFFECTIVE DATE: DECEMBER 2015

TABLE OF CONTENTS **PAGE**

IMPORTANT LINKS
Code 23 Crisis Management
https://lighthouse.ncis.navy.mil/NCIS_Websites/01/crim/opspt/Pages/CrisisManagement.aspx

Employee Assistance Program (EAP)
http://www.foh4you.com

39-1. Purpose. This chapter establishes policy and requirements for developing and executing NCIS office crisis management plans. Guidance is based on references contained in Appendix A. Appendices B through I provide guidance for policy execution.

39-2. Policy. The policy to develop the NCIS office crisis management plans implements procedures consistent with the National Preparedness Guidelines, the National Response Framework, the National Incident Management System (NIMS), Homeland Security Presidential Directive-5, and the Department of Defense (DoD) Installation Emergency Management (IEM) program; references (a) through (e) pertain.

a. The senior NCIS official in each office is responsible for the safety of all personnel and visitors to their facility. NCIS personnel, contractors, and visitors to NCIS office spaces share responsibility for their own personal safety and must cooperate with officials during emergencies. NCIS field offices (NCISFOs), Resident Agencies, and Resident Units will develop crisis management plans to facilitate a coordinated and effective response to hazards and threats affecting their area of responsibility (AOR). It is recognized that some offices are collocated, such as a NCISRA working in the same building as the Field Office or multiple offices working in the same building. In these cases, leadership in those offices will coordinate

and develop one crisis management plan to address responsibilities for those working in the same building.

b. Commanding Officers of Navy and Marine Corps installations have absolute responsibility for the safety and wellbeing of personnel and property on their base or installation. Base and installation commanding officers retain this absolute authority during crisis situations (e.g., when personnel face death or injury or when the security of the installation is in jeopardy) and cannot delegate this responsibility to NCIS personnel, reference (f) pertains.

c. Special agents are authorized to take immediate, direct action to stop active-shooter events and protect and defend themselves and others. Under the inherent right to self-defense, armed and unarmed personnel may also act to protect and defend themselves and others. In overseas locations, NCIS management must ensure personnel operate within the scope of any Status of Forces Agreement (SOFA) or other agreement with the host nation, as they may limit the authorities and protections afforded to NCIS special agents and law enforcement personnel.

d. NCIS management will leverage available NCIS resources and ensure active-shooter training is provided to all NCIS personnel under their supervision. NCIS offices will assist in coordinating active-shooter training to support installation law enforcement personnel per reference (g). NCIS offices must coordinate, train, and exercise procedures with installation law enforcements elements charged with responding to active-shooter events in an effort to mitigate casualties or "blue-on-blue" incidents, as these events are unpredictable and may result in NCIS personnel being the first law enforcement officers (LEOs) on scene during an active event.

e. Per reference (g), NCIS has exclusive responsibility for liaison with federal, state, local, and foreign law enforcement, security and intelligence agencies; commands may pursue liaison activities in support of antiterrorism (AT) matters in coordination with NCIS. NCIS will lead liaison initiatives between commands and other law enforcement agencies to ensure local agencies will provide support services that cannot be supported by command or NCIS personnel. It is the responsibility of the command, with NCIS assistance, to develop response procedures, to include outside agency responsibilities and development of support agreements, as deemed appropriate.

f. Consistent with references (g) and (h), NCIS special agents are authorized to carry NCIS-approved firearms at all times, on and off-duty, and on or off installations, aircraft, and ships. Statutory authority for carrying firearms by NCIS special agents is found in reference (i). References (j) and (k) provide statutory authority for NCIS special agents to execute Federal warrants and make arrests for violations of Federal law. Firearms may be issued to non-special agent personnel who meet requirements specified in references (l) and (m).

g. Reference (n) provides that federal law enforcement officers are involved in a use of force off-duty incident consistent with the provisions of reference (n), they are within the scope of their employment for liability purposes if the officer takes reasonable action to: (1) protect an individual in the presence of the officer from a crime of violence, (2) provide immediate assistance to an individual who has suffered or who was threatened with bodily harm, and (3) prevent the escape of any individual who the officer reasonably believes to have committed in

the presence of the officer a crime of violence. Reference (n) does not apply to NCIS personnel who are not acting in a law enforcement capacity.

h. NCIS policy does not dictate the number of personnel required to intervene in an active-shooter event, as immediate, direct action is necessary to stop the threat. NCIS special agents involved in a tactical response are empowered to decide when to intervene. Because NCIS special agents wear civilian attire both on and off duty, a response requires self-identifying. Body armor with appropriate "POLICE" markings is effective, and responders must ensure they are properly identified and equipped to respond. Responding individuals must attempt to notify the dispatcher, the Incident Command Post (ICP), the incident commander (IC), NCIS supervisor, Multiple Threat Alert Center (MTAC) Watch, and other law enforcement officers before entering an active event to mitigate casualties, as the response typically involves multiple armed personnel. Legal authority and agency policy regarding the use of force will be followed in accordance with references (i) and (m).

i. The following may be acts of terrorism under FBI jurisdiction: active shooter; barricaded subject or hostage; and chemical, biological, radiological, nuclear (CBRN) threats, among other events. NCIS offices must determine jurisdiction in advance of an event to determine response responsibilities on board an installation and the level of involvement by external partners. The policy and procedures for criminal investigations conducted by the criminal investigative organizations of the Department of Justice and DoD are available at reference (o).

j. The use of intercept equipment, including throw phones used by NCIS-trained crisis negotiators, must conform to administrative requirements in reference (p).

39-3. Cancellation. NCIS 3, Chapter 39, dated April 2008.

39-4. Chapter Sponsor. NCIS Criminal Investigations Directorate, Code 23.

39-5. Requirements. NCIS crisis management plans must address response procedures for the hazards and threats identified in Appendices B through F and include a schedule for the annual required NCIS office exercise detailed in Appendix G.

a. Installation integration. NCIS offices will participate in Antiterrorism (AT) and IEM working group meetings, which assist in the development of NCIS crisis management plans. The development of crisis management plans entails coordination with both internal and external stakeholders and aligns with both the IEM and installation AT plan. NCIS will participate in the development of the installation capabilities assessment to ensure NCIS capabilities, requirements, and response expectations are properly understood and included based on NCIS mission requirements.

b. All-hazards concept. NCIS crisis management plans are based on an all-hazards concept, which refers to any natural or manmade situation that warrants action to protect life, property, health, and safety of military members, dependents, and civilians. NCIS crisis management plans must address hazards and threats that could logically manifest in the component's AOR.

c. Active-shooter. The crisis management plan must address NCIS response to active-shooter events in coordination with procedures outlined in the installation AT plan. At a minimum, NCIS involvement for such events includes liaison, advisor to command, intelligence gathering, and investigation. Crisis negotiation may also be provided by NCIS, if the local NCIS agents have the prerequisite training and if the local installation requests NCIS to provide the service. These responsibilities and specific roles for personnel, including the NCIS tactical leader, must be included in the active shooter response appendix of the crisis management plan. An after-action report summarizing and critiquing the event is required and should be expeditiously prepared and directed to NCISHQ (Code 23B). Appendix C provides guidance for plan development and execution of responsibilities.

d. Barricaded subject or hostage. The crisis management plan must address the NCIS response to barricaded subject and hostage events. NCIS involvement for such events is limited to the following general areas: liaison, advisor to command, intelligence gathering, crisis negotiation, and investigation. Crisis negotiation services may be provided by NCIS if available and requested by command. These responsibilities and specific roles for personnel, including the NCIS tactical leader, must be included in the barricaded subject and hostage event response appendix of the crisis management plan. Appendix D provides guidance for plan development and execution of responsibilities.

e. Natural disaster and severe weather. The crisis management plan must address the NCIS response to natural disaster and severe weather events that may occur in the office's AOR and affect operational readiness. The NCIS crisis management plan must provide steps for preparedness, detection, response, and recovery. Plans must identify specific roles and responsibilities for all building occupants, including the senior NCIS official and members to serve as the Emergency Operations Team (EOT), as appropriate, based on the needs of the office. Appendix E provides guidance for plan development and execution of responsibilities.

f. Chemical, biological, radiological, nuclear, explosive (CBRNE) /hazardous materials (HAZMAT). The crisis management plan must address the NCIS response to CBRNE/HAZMAT events that may occur in the AOR and affect operational readiness. Plans must provide steps for preparedness, detection, response, and recovery. Plans must identify roles and responsibilities for all building occupants, including the senior NCIS official and other members to serve as the EOT, as appropriate, based on the needs of the office. NCIS personnel may not enter CBRNE/HAZMAT contaminated areas, nor handle, secure, or transfer contaminated evidence. Once the incident area has been deemed safe or "clear" by CBRNE/HAZMAT teams, NCIS personnel may respond and support first responders in securing the perimeter of the event, maintaining integrity of the crime scene, and assist in preliminary interviews of witnesses and uncontaminated victims. Reference F provides guidance for plan development and execution of responsibilities.

g. Maps. Installation jurisdictional maps must be included in the crisis management plan and provided to law enforcement partners in the office AOR to aid in response planning.

h. Facility floor plans. Floorplans and surveys of key facilities, including those that handle money and may be attractive robbery targets (e.g., on-base banks, restaurants, stores) and

dwellings where domestic violence most frequently occurs (e.g., barracks rooms, on-base housing units) will be included in the crisis management plan and/or be immediately accessible if stored electronically.

i. Communications. The crisis management plan must include a communications plan, equipment requirements, and personnel accountability procedures. NCIS management must ensure DD FM 93s (Record of Emergency Data) for all personnel are current and accessible. Management must ensure all personnel can log into the Navy Family Accountability and Assessment System (NFAAS) to report personnel accountability and are provided with MTAC Watch contact information.

j. Annual exercise. All NCIS offices must conduct one exercise annually based on one crisis event addressed in the crisis management plan. The four-phase exercise entails the discussion phase in the first quarter, the tabletop exercise in second quarter, full-scale exercise in the third quarter, and the critique/remediation in the fourth quarter. This requirement may be achieved through participation in annual installation or regional exercises when NCIS plays a significant role in the exercise. In this case, the phases above may be accomplished outside of the quarterly schedule based on the installation or regions exercise planning schedule. The SAC reviews and approves all NCIS full-scale exercise plans prior to execution. NCIS offices will evaluate the full-scale exercise after completion to address and mitigate vulnerabilities and enhance the effectiveness of the crisis management plan. Appendix G provides guidance for exercise planning and execution.

k. Periodic review. Complete NCIS crisis management plans will be marked "For Official Use Only-Law Enforcement Sensitive." Crisis management plans must be updated to reflect changes to personnel roles/responsibilities or changes to response procedures. Crisis management plans must be reviewed each fiscal year, and additionally as needed, and signed by both the supervisor responsible for the NCIS office and the SAC. Field offices must maintain copies of all NCIS crisis management plans for offices under their purview.

l. Resources. The Code 23 Crisis Management page on Lighthouse contains additional resources for plan development and an example of a thorough crisis management plan.

m. Immediate reporting. NCIS offices must immediately report the following crisis events to the MTAC Watch. Notification may result in the initiation of the MTAC Initial Response Team (IRT) or Crisis Action Center (CAC). MTAC Watch crisis response procedures are detailed in Appendix H.

(1) Terrorist attack on DON personnel or assets.

(2) Barricaded subject or hostage events.

(3) Isolated persons or abducted/missing NCIS personnel and family members.

(4) CBRN/hazmat event.

(5) Significant cyber events immediately affecting warfighting capabilities.

(6) Imminent terrorist attack on DON personnel or assets.

(7) Active-shooter events.

(8) Natural disaster or severe weather events of devastating consequences requiring immediate NCISHQ support to field operations, personnel, and resources.

(9) Movement toward conflict.

(10) Major criminal, terrorism, or counterintelligence investigations (as determined by the appropriate Executive Assistant Director) or those likely to draw media attention where the subject or victim has a DON affiliation.

n. Support services. Appendix I provides information for recognizing the signs of critical incident stress and providing guidance for support services.

APPENDIX A
REFERENCES

(a) Department of Homeland Security, National Preparedness Guidelines, September 2007

(b) Department of Homeland Security, National Response Framework, May 2013

(c) Department of Homeland Security, National Incident Management System, December 2008

(d) Homeland Security Presidential Directive/HSPD-5, Management of Domestic Incidents, February 28, 2003

(e) DoD Instruction 6055.17, DoD Installation Emergency Management (IEM) Program, Incorporating Change 1, November 19, 2010

(f) U.S. Navy Regulations, Chapter 8, The Commanding Officer, 1990

(g) SECNAV Instruction 5430.107, Mission and Functions of the Naval Criminal Investigative Service, 28 December 2005

(h) SECNAV Instruction 5500.29C, 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, August 27, 2003

(i) Title 10 U.S.C. § 1585, Carrying of firearms

(j) Title 10 U.S.C. § 7480, Special agents of the Naval Criminal Investigative Service: authority to execute warrants and make arrests

(k) Title 10 U.S. Code § 1585a, Special agents of the Defense Criminal Investigative Service: authority to execute warrants and make arrests

(l) DoD Directive 5210.56, Carrying of Firearms and Use of Force by DoD Personnel Engaged in Security, Law and Order, or Counterintelligence Activities, April 1, 2011

(m) NCIS-1, Chapter 34, Firearms, Intermediate Weapons and Use of Force, February 2014

(n) Title 28 U.S.C. § 2671, Federal Tort Claims Act

(o) DoD Instruction 5525.07, Implementation of the Memorandum of Understanding (MOU) Between the Department of Justice (DOJ) and Defense Relating to the Investigation and Prosecution of Certain Crimes, June 18, 2007

(p) NCIS-3, Chapter 36, Electronic Interceptions and Electronic Investigative Aids, December 2008

(q) NCIS-3, Chapter 41, Response Protocol for Major Incidents Involving Naval Criminal Investigative Personnel, May 2015

(r) DoD United Facilities Criteria, Security Engineering Physical Security Measures for High Risk Personnel, 8 February 2011

(s) OPNAV Instruction 3500.39C, Operational Risk Management, 2 July 2010

(t) NCIS-1, Chapter 58, Peer Support Program, August 2015

Pages 1185 through 1236 redacted for the following reasons:
- -
(b)(7)(E)

CHAPTER 40
TITLE: FORFEITURE OF PROPERTY
POC: CODE 00L
DATE: JAN 08

40-1. GENERAL

40-1.1. Certain provisions of both federal and some state laws allow the government to seize and "forfeit" property that is either illegal to possess or has been used in a prohibited manner, generally in the furtherance of some illegal activity. Forfeiture is commonly used in drug-related cases, and forfeitable property in this context includes drugs themselves and vehicles, personal property, and even real estate that has been used or intended for use in connection with illegal drug activity. Those provisions, liberally applied, can obviously be a strong deterrent to such activity. An added bonus to law enforcement is that in many cases the property seized and forfeited may be put back into use to further law enforcement activities. Although the Naval Criminal Investigative Service (NCIS) has no authority to enforce any forfeiture statutes on its own, NCIS may in many cases work with agencies that do have such authority, and therefore should be aware of the existence and mechanics of forfeiture statutes.

40-1.2. To "forfeit" may be defined as "to lose, by some error, fault, offense, or crime." As used in most "forfeiture" statutes, and particularly in the Controlled Substances Act (CSA), the term "forfeiture" refers to the process by which the government (federal or state) becomes the owner of private property, without compensation to the owner, as a result of the property having been in some way connected with an illegal act.

40-1.3. The U. S. Constitution requires that in order for the government to deprive a person of his property, due process of law must be followed. Before the government (federal or state) may take private property, it must first correctly follow appropriate legal steps. To satisfy constitutional safeguards, forfeiture of property may be done only pursuant to a statute or law that declares a particular property, or class of property, forfeitable.

40-1.4. Forfeiture statutes may be classified as either civil or criminal. As the terminology implies, the distinction is that criminal forfeiture is the taking of property as punishment for the conviction of its owner of some underlying criminal offense, while civil forfeiture is an administrative remedy, which is independent of any criminal proceedings.

40-2. CRIMINAL FORFEITURE. The Uniform Code of Military Justice (UCMJ) has no

provision for the forfeiture of property (other than pay and allowances) as a criminal penalty. Other federal laws, and many state laws, do provide for forfeiture of certain specified properties when the owner is convicted of a crime. Forfeiture provisions are included as a part of the indictment. Should the charged individual be found not guilty, the property will not be forfeited. Criminal forfeiture is more difficult to accomplish, as it places a substantial burden of proof on the government. Since it is a criminal proceeding, the standard of proof is "beyond a reasonable doubt." The government's burden of proof for a civil forfeiture is significantly less.

40-3. CIVIL FORFEITURE

40-3.1. Civil forfeiture statutes frequently distinguish between property which may be forfeited summarily, so-called "contraband per se," the mere possession of which is generally prohibited, and "derivative contraband," or property which ordinarily would be legal to possess, but becomes forfeitable because of the use, or intended use, of that property. Examples of contraband per se are heroin, automatic weapons, and counterfeit currency. On the other hand, an automobile and laboratory equipment are innocent items themselves, but if the automobile is used to transport illegal drugs or the laboratory equipment is used to manufacture drugs, they may be forfeitable to the government because of their use in the furthering of illegal purposes.

40-3.2. Unlike criminal forfeiture, civil forfeiture does not require a criminal conviction. Although a criminal prosecution may arise out of the same incident, a civil forfeiture may take place although the person whose property is forfeited is not prosecuted, and that forfeiture will generally stand even though the person may later be tried and found not guilty of the incident.

40-3.3. Also unlike criminal proceedings, civil forfeiture is directed at the thing to be forfeited, rather than at a particular person. The constitutional safeguards required are much lower. When possession of an item is declared by statute to be illegal (contraband per se) the person possessing such an item has no legal property rights in that item (with rare exceptions) and, if discovered, the item will be confiscated (seized and forfeited) with little or no "due process" required. On the other hand, where an item is not in and of itself illegal, but is only rendered forfeitable because of a prohibited use or intended use, certain steps must be taken, and the property owner does have certain rights associated with the forfeiture.

40-3.4. The burden of proof threshold in civil forfeiture is probable cause to believe that the property is forfeitable.

40-3.5. Once such probable cause has been shown, the burden shifts to the person contesting the forfeiture to show by a preponderance of the evidence that the property was not used or intended to be used in a prohibited manner, that an exception to the statute should apply, or that remission or mitigation of the forfeiture should be considered. Remission is a "pardoning" of property civilly forfeited, and generally requires a showing of lack of fault or lack of knowledge by the party seeking remission. Mitigation in this context involves allowing a party to pay a money penalty in order to regain forfeited property.

40-3.6. The statute of limitations for most civil forfeiture proceedings is five years from the date the probable cause to believe the property was used in a prohibited manner was discovered (or should

have been discovered from available information). In many cases, it is possible to go back and seek forfeiture of assets identified in past, and even closed, investigations.

40-3.7. Technically, forfeiture occurs at the moment of the illegal use of the property. Once the property has been used in a manner making it forfeitable by statute, the title instantly passes to the government. Once the government has this equitable title (even though no forfeiture proceedings have been instituted, and in fact the illegal action may not yet have been discovered), the former owner cannot defeat forfeiture by selling or otherwise disposing of the property.

40-4. CIVIL FORFEITURE UNDER 21 USC 881

40-4.1. Property subject to forfeiture. The forfeiture statute most commonly used is contained in Chapter 13 of Title 21 United States Code (USC), DRUG ABUSE PREVENTION AND CONTROL (hereafter referred to as the Controlled Substance Act, or CSA). The forfeiture provisions of that Act are found at 21 USC Section 881, which provides that the following categories of property shall be subject to forfeiture to the United States "and no property right shall exist in them."

a. Controlled substances that have been illegally manufactured, distributed, or acquired;

(1) Schedule I and II substances are considered contraband per se and are subject to forfeiture summarily. All other controlled substances require probable cause to believe the substance was illegally manufactured, distributed, dispensed, acquired, or possessed.

b. Raw materials, products, and equipment of any kind which are used, or intended for use, in illegally manufacturing, compounding, processing, delivering, importing or exporting any controlled substance;

(1) Common examples of this type of property include glassware, chemicals, cutting materials and implements, scales, pumps and radios. Anything tangible may be included in this category except land, buildings, money, and "conveyances," all of which are covered under other parts of the statute. Equipment used or intended to inject, inhale, or otherwise ingest a controlled substance ("paraphernalia") is not included under this section.

c. Property which is used, or intended for use, as a container for property described in paragraphs a and b;

(1) Almost anything used to hold, wrap, package, store, or conceal forfeitable drugs can be included in this section (except vehicles, land, or buildings). Cans, bags, bottles, luggage, attaché cases, envelopes, lockers, musical instruments, stereo gear, statues, and other art work have been so used. Again, either actual use or intent to use as a container for controlled substances is all that need be shown to justify commencing forfeiture proceedings.

d. Conveyances, including aircraft, vehicles, or vessels, which are used or intended for use, to transport, or in any manner to facilitate transportation, sale, receipt, possession, or concealment of property described in paragraphs a or b;

(1) This subsection of the CSA forfeiture provisions can be expected to have the greatest impact on NCIS. All vehicles entering a military installation and connected in any way with illegal drugs are primary civil forfeiture targets.

(2) Anything capable of carrying people or goods is a "conveyance" under this section. This includes automobiles, motorbikes, motorcycles, mopeds and even bicycles. Mobile homes or trailers that are used or are readily capable of being used as true mobile homes are considered to be conveyances. HUD-defined "manufactured housing," installed at fixed locations on permanent or semi-permanent foundations, even though located on government property, should probably be considered real estate, and is covered under another section.

(3) "Appurtenances" (objects which have a purpose related to the conveyance, are generally attached, and which are generally considered a permanent part of the conveyance) are also forfeitable. Spare tires, radios, jacks, hubcaps, mirrors, seat covers and floor mats are appurtenances and are forfeitable with the conveyance. On the other hand, personal property found within a forfeitable conveyance is not automatically forfeitable unless it is an appurtenance or is forfeitable in its own right.

(4) By statute, transportation of controlled substances for any prohibited purpose, in any amount, subjects a vehicle to forfeiture. Because possession of even small amounts has a much more significant impact on military installations, contact should be made with the local field offices of the Federal Bureau of Investigation (FBI) and Drug Enforcement Agency (DEA) to determine what amounts will be considered significant for their forfeiture procedures, keeping in mind the unique considerations involving controlled substances on military installations.

(5) Conveyances used to facilitate a prohibited activity are also forfeitable, even though such vehicles may contain no illegal drugs themselves. A conveyance "facilitates" a violation when it "makes the violation easier or less difficult." Vehicles used as escorts, decoys, and pilot vehicles or for counter-surveillance are forfeitable. A vehicle used as a meeting place to arrange a drug deal or to convey money to be used in a drug deal is forfeitable. Court decisions have held forfeitable a vehicle used to facilitate the movement of narcotics proceeds to money launderers; aircraft used to transport conspirators to a site for exchange of controlled substances; and a truck which was used to carry tools used to grow marijuana.

e. Books, records, and research, including formulas, microfilm, tapes, and data which are used, or intended for use, in violation of the CSA;

(1) Formula, microfilm, tapes, data and record books made and kept by drug violators are forfeitable. However, books of general distribution and drug-related literature are constitutionally exempt from forfeiture by the First Amendment of the Constitution.

f. Moneys or other things of value furnished or intended to be furnished in exchange for a controlled substance, all proceeds traceable to such an exchange, and all moneys, negotiable instruments and securities used or intended to be used to facilitate any violation of the CSA;

(1) Clearly, direct observation of exchanges can establish that particular currency or property was exchanged or intended to be exchanged for controlled substances. In addition, actions or statements may indicate that property was or was intended to be exchanged for drugs, rendering the property forfeitable. For example, in a situation where a potential buyer is observed to produce a checkbook indicating the amount negotiated for the sale, the checkbook and the money in the account are both subject to forfeiture. Circumstantial evidence that an illegal exchange took place or was intended may provide sufficient probable cause to begin forfeiture proceedings.

(2) The proximity of money and drugs found together may, in some cases, provide sufficient probable cause to believe the money is proceeds of illegal activity. Where only small amounts of money are found, the probable cause to believe the two are related is lessened, since the possession of small amounts of money for innocent purposes is common. Even small amounts of money found on a known drug trafficker may be considered to be innocent, absent other evidence to the contrary. However, because of the "cash and carry" nature of the drug business, the courts have consistently upheld forfeiture of large, unexplained quantities of money found in the proximity of illegal drugs or other evidence of trafficking, or found on the person of a known drug trafficker. Large sums of money raise the probability that the funds are involved with such trafficking, rather than for personal use.

(3) Proceeds. If something exchanged for illicit drugs is later sold, traded or otherwise disposed of, everything received in its place is considered "proceeds" of the original drug exchange. If these proceeds are disposed of, everything received in their place is considered "proceeds" of the original exchange. So long as these changes of property can be traced and the proceeds described with reasonable accuracy, they are subject to civil forfeiture. "Proceeds" are whatever is received when an object is sold, traded, exchanged or otherwise disposed of. The definition of “proceeds” is not limited to money.

g. Real property, including improvements, which is used or intended to be used in any manner to commit, or to facilitate the commission of, a violation of the CSA;

(1) The statute specifically states that "appurtenances or improvements" to real estate are included within this section. Land, buildings, leases of real property, easements, joint and common ownership rights, partnership and corporate holdings, and more-or-less permanently-affixed mobile homes/manufactured housing are among the kinds of real estate interests which may be forfeitable. A real estate interest "facilitates" a drug violation if it makes the offense easier to commit or is otherwise significantly connected to the offense.

(2) In order for a real estate interest to be forfeitable under this section, the illegal use, intended use, or illegal facilitation of a drug offense must have taken place on or after 13 October 1984, the effective date of the amended legislation. However, real estate that is "proceeds" of a pre-13 October 1984 drug violation is forfeitable under the proceeds provision.

h. Controlled substances possessed in violation of the CSA.

This subsection was added to remedy the omission of illegal possession in subsection a.

40-4.2. Exceptions. There are certain exceptions to the above.

a. In most cases, common carriers are exempted from forfeiture simply because they are used by a passenger in a prohibited manner, since they are by law required to make themselves available to the general public. If the owner or person in charge had actual knowledge of the illegal activity, or was negligent in its prevention, even those vehicles may be subject to forfeiture.

b. A stolen vehicle is not generally subject to forfeiture.

c. An "innocent" owner or lien holder of a secured interest in property may be protected to the extent of his/her ownership interest.

d. In some cases, even when property is forfeitable, the responsible agency may grant a remission or mitigation of the forfeiture (see paragraph 40-03.5). However, any exceptions, remissions, or mitigation must be granted by the forfeiting agency. All requests and/or inquiries must be directed to the forfeiting agency.

e. When investigation indicates that there is probable cause to believe that property is forfeitable, even though it appears that an exception may apply, or remission or mitigation may be requested, the forfeiting agency should still be advised of the identified property and the decision to proceed or not proceed with forfeiture left to that agency.

40-4.3. Who may enforce civil forfeiture under the CSA

a. The CSA provides that the U.S. Attorney General shall designate agencies within the Department of Justice to accomplish CSA civil forfeiture. The FBI and DEA have been so designated. NCIS has not been designated as an agency authorized to accomplish civil forfeiture under the CSA.

b. While NCIS has no authority to seize property for forfeiture purposes and may not seize any property solely for the purposes of civil forfeiture, there will be many instances when property seized as evidence in an NCIS investigation will be recognized as property subject to civil forfeiture. In other cases, NCIS investigations will identify property, which, although not subject to seizure by NCIS, is forfeitable under the provisions of the CSA. In such cases, an authorized agency may adopt probable cause developed by NCIS to proceed with seizure and forfeiture of the identified property.

c. Posse Comitatus considerations. The Posse Comitatus Act (18 USC Section 1385) specifically prohibits the Army and Air Force from enforcing civilian laws. Although the Navy and Marine Corps are not so prohibited by statute, the provisions of the Act have been adopted by the Department of the Navy (DON) as a matter of policy, as defined in SECNAVINST 5820.7C, which provides the following:

(1) Civilian special agents of the NCIS, when performing criminal and security investigations, are not considered to be under the direct command and control of a military officer, and therefore are not subject to the prohibitions of posse comitatus.

(2) Further, because the prohibition is a matter of policy rather than statute, the Secretary of the Navy may grant exceptions to that policy in appropriate cases. In most instances, these require prior approval, as spelled out in the referenced instruction, but may extend to use of DON equipment, facilities, or personnel.

(3) Military personnel, including Reservists assigned to support NCIS activities, are prohibited from directly assisting civilian law enforcement activities, and should not perform duties related solely to the assistance of civil law enforcement, including matters related to civil forfeiture. So long as such tasking is directed to a valid NCIS investigation, the fact that information incidental to the investigation is later furnished to a civilian law enforcement agency does not violate the Act or SECNAVINST 5820.7C.

40-5. FORFEITURE PROCEDURES UNDER 21 USC 881

40-5.1. 21 USC Section 881 provides that any property subject to forfeiture under its provisions may be seized:

a. Upon process issued by any U.S district court; or

b. Without such process when:

(1) The seizure is incident to an arrest or a search under a search warrant or an inspection under an administrative search warrant;

(2) The property subject to seizure has been the subject of a prior judgment in favor of the United States in a criminal injunction or forfeiture proceeding;

(3) The Attorney General has probable cause to believe that the property is directly or indirectly dangerous to health or safety; or

(4) The Attorney General has probable cause to believe that the property is subject to civil forfeiture.

c. In the event of seizure under (3) or (4), above, the government must promptly institute forfeiture proceedings, which may be either summary or judicial.

40-5.2. Proceedings After Seizure

a. Property valued at $100,000 or less may be forfeited by first giving notice to "each party who appears to have an interest in the seized article." Any interested party may file a claim and post a bond of the lesser of $5000 or 10% of the article's value ($250 minimum). If no claim is filed or bond posted within 20 days, the government may declare the property forfeited and may proceed to dispose of the property.

b. If a claim and bond is filed within the 20-day period, or the property is valued at more than

$100,000, the matter must be transmitted to the U.S. Attorney for the district in which the property was seized, for the institution of proceedings to condemn the property.

40-5.3. Although there is no minimum statutory value for property to be forfeited, in actual practice the agencies involved discourage forfeiture of property (other than contraband per se) under certain minimum values unless the property is somehow of unique value.

a. Property value guidelines. At the present time, the guidelines followed by both the FBI and DEA for value of forfeitable property are as follows:

(1) $10,000 for real property

(2) $5,000 for aircraft or vessels

(3) $2,500 for vehicles

(4) $1,000 for all other property

b. The value to be considered is the equity value of the property (the appraised value of the property less the value of all outstanding liens). The forfeiting agencies will not generally forfeit property in poor condition, which will require extensive repairs or upkeep, or which is perishable. Additionally, the agencies normally will not forfeit property when only small quantities of controlled substances are involved. Finally, agency guidelines require consideration of claims or potential claims of "innocent ownership" which might as a practical matter prevent forfeiture procedures from being worthwhile.

c. Because of the special problems presented by drug abuse on military installations, it is recommended that liaison be made with the local field offices of both the FBI and DEA in order to determine the quantity thresholds to be used in such cases. Because of the inherent dangers posed to military installations, the presence of illegal controlled substances in any amount (or at least in smaller amounts than would be tolerated in the civilian community) should be considered sufficient to warrant forfeiture in cases involving illegal substances on a military installation.

40-5.4. After property has been declared forfeited, the government may dispose of the property in a number of ways. It may order the property destroyed; it may sell the property; if the property is suitable, it may be retained for law enforcement purposes by the forfeiting agency; it may be transferred to any other agency, federal, state or local, for appropriate official use. The property may be so transferred whether or not the other agency had any part in the forfeiture of the property. However, in cases where another agency was involved in the forfeiture, it is the policy of the Justice Department and the Attorney General to give special consideration to "equitable" transfer of such property to the agency, which contributed to the actual forfeiture, upon request by the contributing agency.

40-6. TRANSFER OF FORFEITED ASSETS

40-6.1. The policy of the Department of Justice is to manage its asset forfeiture program in a

manner designed to enhance federal, state, and local cooperation in law enforcement efforts, especially in the area of drug activity. As a consequence, the Attorney General has issued guidelines designed to ensure transfer of forfeited property to reflect generally the contribution of other federal, state and/or local agencies that participated directly in any of the acts, which led to seizure, or forfeiture of the property.

40-6.2. Property forfeited either administratively or pursuant to a court order may be transferred.

40-6.3. Assets that may be transferred to participating agencies must be used in furtherance of law enforcement activities. Seized funds may be transferred to state and local agencies but only tangible assets may be transferred to a federal agency (including NCIS). Seized vehicles constitute the most commonly transferred assets, but a variety of forfeited items may be utilized for law enforcement purposes.

40-6.4. Requests for Transfer of Forfeited Assets

a. An agency desiring the transfer of a forfeited asset must submit a written request to the local or regional office of the agency that is (or will be) responsible for processing the forfeiture. The request should be submitted within 30 days following the seizure for forfeiture, but in any event no later than the date of forfeiture or the disposition of the property, whichever is later. The date for the request is calculated from the date the property is seized for forfeiture, not necessarily the date that the property may have been seized by NCIS in the course of an investigation for evidentiary purposes. However, since the forfeiting agency has priority to retain the asset itself, and any other participating agency may also request transfer of the property, the early submission of any such request is strongly recommended.

b. A request for transfer of forfeited property must be certified to be true and correct, and must contain the following information:

(1) Identification of the property for which the claim is made;

(2) Details regarding NCIS participation, including the amount of money and manpower expended in pursuing the case;

(3) A statement of the intended law enforcement use for the property;

(4) A designation of the proper fiscal entity to which disbursements can be made; (note that this will seldom, if ever, apply, as federal agencies are only eligible for transfer of tangible assets).

(5) A designation of the proper person to whom transfer documents should be delivered by the United States;

(6) A designation of the proper person to whom possession should be delivered;

(7) A statement by an appropriate legal officer indicating that the transfer is not prohibited under the applicable federal, state or local law;

(8) In instances of a joint application by several federal, state or local agencies, the relative share of each federal, state or local agency;

(9) A statement that all fees and expenses necessary to effect transfer of title will be paid by or on behalf of the requesting agency not later than the time of transfer; and

(10) An assurance that, if requested to do so, a report will be provided as to the actual use of any transferred property.

c. In most instances, the forfeiting agencies and the U.S. Attorney General's office will require completion of form DAG-71, which requires the information listed above.

40-6.5. The field unit receiving the request must then prepare an evaluation of the degree of assistance provided by NCIS in the underlying investigation. In determining the "equitable share" for a participating agency, the governing factor is the time and effort contributed by each agency participating directly in the investigation or other law enforcement activity that led directly or indirectly to the seizure or forfeiture of the property. If the effort of the forfeiting agency itself is ten percent or less, an allocation of ten percent will be made to the forfeiting agency to compensate for its administrative role. For purposes of practicality, the "ten percent rule" does not apply to assets that are not readily divisible.

40-6.6. The recipient agency must pay all liens and mortgages on forfeited property pursuant to court order or an order of remission or mitigation prior to the transfer of such property.

40-6.7. The recipient agency may be required to pay direct expenses pertaining to the seizure and forfeiture prior to the transfer of the property.

40-6.8. In some circumstances, the United States Marshals Service may transfer tangible property to any requesting federal agency that did not participate in the acts that led to a seizure or forfeiture.

40-6.9. Points of contact for all matters involving possible forfeitures or possible equitable transfer of assets will be the local field offices of the FBI and DEA. The United States Marshals Service, which acts as custodian of property forfeited to the United States, is the point of contact for the transfer of assets that have already been forfeited. Liaison should be made in advance, policy matters worked out, and regular points of contact established so that when a potential forfeitable asset is recognized, whether or not an equitable transfer request is to be made, the information can be provided to the forfeiting agency early on.

40-7. NCIS PARTICIPATION IN THE CSA FORFEITURE PROCESS

40-7.1. NCIS participation in the forfeiture process begins with the identification of assets that may be subject to forfeiture.

40-7.2. As soon as such property has been identified, probable cause to believe it has been used in a manner covered by the forfeiture statute should be documented. Consideration should be given to

informally advising the appropriate agency of the possible existence of such property at an early point.

40-7.3. After it has been determined that probable cause exists, additional investigation should be done, where feasible, to determine the value of the property and the existence of liens and any obvious claims to "innocent ownership." In community property states, the potential claims of spouses should always be kept in mind. While the burden remains on the claimant to show ignorance of the prohibited use and that the claimant took reasonable precautions to prevent the prohibited use, it is nevertheless advisable to keep potential claims in mind, especially if equitable transfer of the asset is being considered.

40-7.4. If investigation reveals that funds were received by a suspect which would have been forfeitable, but which have since been spent, if possible attempt to identify tangible assets traceable to those funds.

40-7.5. If it is determined that the property meets the guidelines for the agency which will actually accomplish the forfeiture, that agency should immediately be contacted and advised. A Report of Investigation, Results of Investigative Activity, or a memorandum citing the proper probable cause should accompany the request. It is expected that local conditions and practice will dictate the agency best suited to accomplish the forfeiture, and that liaison will be made locally as to the precise procedures to be followed after forfeitable property is identified.

40-7.6. If the identified property is in NCIS custody, a determination should be made as to whether the property will be needed for evidentiary purposes, or whether it is to be released. Property ordinarily should not be seized or retained solely for purposes of civil forfeiture. If the property is in custody but is of a kind that would ordinarily be released to its owner, the forfeiting agency should be advised that the property will only be held for a reasonable time, after which it will be returned to the owner.

40-7.7. If it appears that an equitable transfer of the property to NCIS may be desired, a request should be prepared in accordance with the guidelines set out in section 40-6, and submitted to the forfeiting agency.

40-8. OTHER FORFEITURE STATUTES. While forfeiture under the Controlled Substance Act will likely most often apply, forfeiture of property is authorized under a number of state and local statutes. No attempt will be made to list state statutes, but it is useful to be familiar with those that may apply in your area.

NCIS-3, CHAPTER 41
RESPONSE PROTOCOL FOR MAJOR INCIDENTS INVOLVING NAVAL CRIMINAL INVESTIGATIVE SERVICE PERSONNEL
DATE: MAY 2015

TABLE OF CONTENTS **PAGE**

References:

(a) NCIS Manual 1, Chapter 5, Inspector General Matters, September 2007
(b) 18 U.S. Code § 3261-67, Military Extraterritorial Jurisdiction Act (MEJA)
(c) DoD Instruction 5525.11, Criminal Jurisdiction Over Civilians Employed by or Accompanying the Armed Forces Outside the United States, Certain Service Members, and Former Service Members, 3 March 2005
(d) NCIS Manual 3, Chapter 7, Rights Warnings and Self-Incrimination, March 2013

41-1. Purpose. This chapter establishes NCIS policy and procedures for criminal and administrative investigations of major incidents involving NCIS personnel. These policies and procedures are to be used when a major incident involves NCIS personnel as "incident employees" or victims of a fatal or serious injury, when an employee(s) is missing as a result of a kidnapping, or when an individual in NCIS custody is seriously injured or dies. An "incident employee" is an NCIS employee who is involved in a line-of-duty shooting incident or whose actions resulted in serious injury. These policies apply to NCIS special agents in both on-duty and off-duty status. For non-special agent personnel, these policies normally apply to on-duty situations. Major incidents include the following:

a. Intentional or accidental shootings or use of force incidents resulting in injury or death.

b. Assaults resulting in serious injury to or by NCIS personnel.

c. Disappearance of an NCIS employee due to kidnapping or other crime.

d. Fatal or serious injuries to a person in NCIS custody, including serious injuries sustained to passengers in an NCIS vehicle.

e. Vehicle collisions and other accidents in which a serious injury occurs.

41-2. Policy

a. There are many legal, organizational, and personal implications involved in a major incident, and it is NCIS policy to ensure a thorough and unbiased investigation is conducted of each major incident involving an NCIS employee, in accordance with reference (a).

b. In any major incident, the investigative needs of NCIS and other law enforcement agencies take precedence. This chapter provides procedural guidelines for the management and investigation of a major incident. Appendix A provides guidance on the roles and responsibilities of NCIS personnel involved in managing the incident scene. The Emergency Notification Protocol is provided in Appendix B. The specific duties assigned to an incident employee(s) are contained in Appendix C. The responsibilities of the SAC (or designee) are contained in Appendix D. The On-Scene Supervisor Checklist is contained in Appendix E, and the Companion Agent Checklist is provided in Appendix F.

c. When an NCIS employee is involved in a major incident, the NCIS Office of the Inspector General (Code 00I) will initiate an investigation under case category 2B-Internal Personnel Inquiry. Code 00I or its designee will conduct a thorough investigation of the involvement of the NCIS employee(s) in the major incident. The investigation may be used to determine the need for improvements in NCIS policies, procedures, equipment, and supervision. These are the objectives of the NCIS investigation:

(1) Determine any criminal liability of the NCIS employee(s) or others.

(2) Determine whether NCIS employee(s) violated NCIS policies and procedures.

(3) Prepare for any administrative or civil litigation that may result from the incident.

(4) Obtain details of the incident to inform NCIS, DON, and DoD management.

d. NCIS employees should be aware that due to jurisdictional factors, another law enforcement agency (local, Federal, or foreign) may conduct a separate investigation. Although the internal personnel inquiry may be separate, NCIS will normally coordinate aspects of any criminal investigation with the law enforcement agency that has investigative jurisdiction.

41-3. Cancellation. NCIS-1, Chapter 41, dated September 2009.

41-4. Chapter sponsor. The Office of the Inspector General (Code 00I).

41-5. Jurisdiction

a. Criminal investigation. The law enforcement agency that has criminal investigative jurisdiction in a major incident is dependent on applicable laws, agreements, and territorial jurisdiction. Jurisdiction does not change because a Federal agent is involved. The following

guidelines generally apply in determining primary investigative jurisdiction:

(1) Local authorities have jurisdiction and will normally conduct an investigation when an incident occurs off a military reservation or on a military reservation where the Federal Government has only proprietary legal interest. Usually in this circumstance, an NCIS employee(s) will be interviewed if he or she was involved in or witnessed the event.

(2) The Federal Bureau of Investigation (FBI) has criminal investigative jurisdiction when an incident involves a civilian NCIS employee as a suspect, and the incident occurs on a Naval installation in the United States or its territories and the Federal Government has concurrent or exclusive jurisdiction. The FBI may elect to waive jurisdiction to NCIS. However, the FBI must be promptly notified and a decision obtained. NCIS has criminal investigative jurisdiction if the incident involves a military NCIS employee and other military personnel are involved.

(3) In overseas locations, the provisions of any status of forces agreement or other agreement with the host nation determines which agency has criminal investigative jurisdiction. NCIS may have jurisdiction, depending on the provisions of the status of forces agreement. All personnel should be familiar with the provisions of any agreement with the host nation as it pertains to criminal investigations.

(4) Reference (b) establishes jurisdiction in U.S. Federal courts over civilians employed by or accompanying the Armed Forces outside the United States, certain Service members, and former Service members who engage in acts outside the United States that if done in the United States would be punishable by more than one year imprisonment. Reference (c) provides for the implementation of this law.

b. Administrative inquiries. Any agency may conduct an administrative investigation to determine whether any employee violated its policies or procedures, determine improvements that may be necessary, and prepare for administrative or civil litigation. For NCIS, the findings of an internal personnel investigation normally satisfies both the criminal and administrative objectives.

41-6. Legal issues. NCIS employees who witness a major incident are obligated to cooperate with investigating authorities and answer questions truthfully pertaining to the performance of their official duties. However, an incident employee(s) is not compelled to make any incriminating statement or answer incriminating questions during a criminal investigation. With prior approval of a prosecution authority, an incident employee(s) may be compelled to answer all work-related questions truthfully during an administrative inquiry; however, the compelled statements cannot be used in a criminal proceeding. The following guidelines pertain:

a. Investigation by local and other U. S. authorities. Civilian NCIS employees involved in a major incident, particularly a shooting, should anticipate a criminal investigation by another law enforcement agency, as NCIS likely would not have primary investigative jurisdiction.

(1) It is recommended that an incident employee(s) decline to be interviewed by another agency regarding participation in the incident until having had an opportunity to consult with an NCIS supervisor. The recommendation to decline the interview should not preclude an incident

employee(s) from providing basic information to authorities who are attempting to apprehend an at-large suspect.

(2) NCIS employees may be advised of their rights against self-incrimination and subpoenaed to a grand jury, coroner's inquest, or court proceeding. Employees share the same protection as other citizens under the U.S. Constitution and may not be compelled to make self-incriminating statements during a criminal investigation or proceeding. As U.S. citizens, NCIS employees have the right to counsel and protection against unreasonable searches and seizures.

b. Investigation by foreign law enforcement authorities. In overseas locations where a foreign law enforcement agency has primary investigative jurisdiction, NCIS employees should decline to answer questions from foreign officials without first consulting with legal counsel, as the legal rights and repercussions may be substantially different than those under U.S. law. Initially, legal counsel should be available through the U.S. embassy or consulate.

c. Code 00I or designee investigation. During an NCIS internal personnel inquiry, NCIS employees will be provided the appropriate civilian or military rights warning under the same circumstances required for all civilians and Service Members, see reference (d). NCIS employees may exercise the same constitutional rights afforded all citizens when asked incriminating questions or when provided suspect warnings.

(1) One of the objectives of an internal personnel inquiry is to determine criminal liability of the NCIS employee. The employee should be aware that if criminal liability is established, NCIS is obligated to provide the results to the appropriate prosecuting authority for prosecutorial decision.

(2) During an internal personnel inquiry, Code 00I may decide the investigation is strictly administrative in nature. This decision is usually based on a declination of prosecution, lack of facts substantiating criminal liability on the part of the NCIS employee, or lack of criminal investigative jurisdiction. When a civilian NCIS employee has already declined to answer incriminating work-related questions, the employee will be informed that the investigation is administrative in nature and will be offered an additional opportunity to answer the work-related questions truthfully. If the NCIS employee continues to decline to answer the question(s), the employee will be provided a civilian employee administrative warning. This warning compels the employee to respond truthfully to questions directly related to the employee's official duties or face disciplinary action for failure to comply, which could result in the employee's removal from employment, as outlined in reference (d). Compelled responses cannot be used in a subsequent criminal proceeding.

d. Civil liability. An NCIS employee may be subject to lawsuits in a State court on charges of alleged negligent or wrongful acts, or omissions committed in the course of official duties. In such an event, the Department of Justice may move the case to a Federal court. In this circumstance, the Government ordinarily provides legal representation.

(1) An employee also may be sued in Federal court on charges of allegedly violating a person's constitutional rights or on charges pursuant to a specific Federal statute authorizing recovery of money damages. The Government will ordinarily defend such a suit, though the Government has no authority to pay monetary damages assessed against the employee. Among the

defenses available to the employee is qualified immunity, which can result in a dismissal before trial or constitute a legal or factual defense at trial. This defense is established by showing that the employee's conduct did not violate clearly established statutory or constitutional rights, which a reasonable person would have known at the time the action occurred.

(2) Under the Federal Tort Claims Act, a suit may be filed against the Government for alleged, negligent, or other wrongful acts, or omissions committed by the employee during the course of employment. Because the Government is the defendant, the Government will defend the case and be responsible for any compensatory judgment or settlement. In the event that both the NCIS employee and the Government are named as defendants, the Government will provide for the defense and pay any compensatory judgment or settlement entered jointly against the United States or its employee. In the event that punitive damages are assessed against the employee for gross negligence, the employee alone bears responsibility.

Pages 1253 through 1265 redacted for the following reasons:
- -
(b)(7)(E)

CHAPTER 42
TITLE: MISSING PERSONS (CATEGORY 7M)
POC: CODE 23A
DATE: OCT 08

42-1. DISCUSSION

42-1.1. General. Missing Person (Case Category 7M) investigations involve a disappearance in which foul play is suspected, or a disappearance involving unusual or suspicious circumstances. These investigations are initiated when a military member or some individual in his/her immediate family suddenly disappears without explanation, leaving all personal belongings, bank account, etc., intact.

42-1.2. Definitions

a. Unauthorized Absence (UA)/Absence Without Leave (AWOL): A member of the armed forces who, without authority, fails to go to his place of duty at the time prescribed, or departs from that place, or absents himself from his unit, organization or place of duty at which he is required to be at the time prescribed.

b. Desertion: A member of the armed forces who, without authority, goes or remains absent from his unit, organization, or place of duty with the intent to remain away permanently.

c. Fugitive Investigation: Investigation of a person who flees to avoid prosecution for a crime or to avoid giving testimony in any criminal proceeding.

d. Missing Person Investigation: Investigation of the unexplained disappearance of an individual where foul play, unusual or suspicious circumstances are alleged.

42-1.3. Criminal Law/Jurisdiction

a. Uniform Code of Military Justice (UCMJ). Crimes of this category are potentially violations of the UCMJ, along with consideration for attempts and conspiracies:

Article 85 (Desertion)
Article 86 (Absence Without Leave)

An individual who is being investigated as a Missing Person may be the victim or suspect of another category of offense punishable under the UCMJ.

b. Federal Laws/US Code (USC). An individual being investigated as a Missing Person may be the victim or suspect of other crimes enumerated under the federal code.

c. State Criminal Law. An individual being investigated as a Missing Person may be the victim or suspect of other crimes enumerated under the state's penal code.

42-2. POLICY AND GUIDANCE

42-2.1. NCIS Authority. NCIS authority and jurisdiction to investigate this category of offenses is derived from SECNAVINST 5430.107 (28DEC05). DoD Instruction 5525.07 implements the Memorandum of Understanding (MOU) between the Department of Justice and the DoD criminal investigative organizations. The MOU provides policy and guidance for criminal investigations when both departments have jurisdiction.

42-2.2. NCIS Responsibility. The investigating agent must be aware of the potential involvement of homicide, kidnapping, suicide, fraudulent schemes, desertion, absence without leave, and accidental injury or death in Missing Person cases. Requests for investigative assistance can originate from the involved command, concerned relatives, or other law enforcement agencies.

42-2.3. NCIS has jurisdiction in Missing Person investigations due to the possible major criminal offenses that may be involved. SECNAVINST 5430.107 states that the command shall promptly provide available information to NCIS for investigation regarding the disappearance of a command member, which may suggest foul play.

42-2.4. Inasmuch as desertion is a major criminal offense in the UCMJ, NCIS has jurisdiction. However, as a matter of policy, this offense and that of Unauthorized Absence (UA) should be handled by command assets, absent some urgent or unique circumstance which would indicate that a Missing Person investigation is warranted.

42-2.5. In the absence of clear-cut evidence indicating a specific crime is involved, the 7M case category will be utilized to investigate the disappearance of a person if one of the following circumstances applies:

a. Is missing or lost at sea.

b. Is missing under circumstances indicating that his/her physical safety is in danger, which may be inferred based upon the young age of the missing child and/or any medical conditions or impairments of the individual.

c. Any person who is missing and is mentally/physically disabled so as to subject himself/herself or others to personal danger.

d. Where foul play is suspected or a disappearance involving unusual or suspicious circumstances; or when the absence is inconsistent with the individual's established patterns of behavior and the deviation cannot be readily explained.

e. Missing children (see section 42-4.5 below for further guidance).

42-2.6. Upon initiation of a missing persons investigation (7M), NCISHQ Code 23B DSI/SI (Missing Persons) desk officer, should be info copied on the ROI (OPEN). The NCISHQ Code 23B DSI/SI (Missing Persons) desk officer will make a determination if the investigation will be monitored as an SI (Special Interest) or DSI (Director's Special Interest) investigation. Coordination between NCISHQ Code 23B DSI/SI and the case agent should occur as appropriate and necessary. All subsequent ROI (INTERIM)s should info copy NCISHQ Code 23B DSI/SI (Missing Persons) as appropriate.

42-2.7. Upon completion of all logical leads, a ROI (INTERIM), to include as exhibits (if available) legible copies of the missing person's photograph, fingerprints, and dental record, will be forwarded to NCISHQ Code 24B3, Forensic Science and Biometrics Division. Missing Persons investigations will remain open until the status of the missing person is determined. Field offices may request a Missing Persons Review Board (MPRB) examination of the investigation if all leads have been exhausted. See section 42-2.10 below for further explanation.

42-2.8. If the Missing Person investigation develops into a specific crime, the case category shall be changed appropriately. If it is determined that the missing person is in actuality a fugitive, then the case category will be changed to a Fugitive Investigation (7F); see NCIS-3 Chapter 2 (Fugitive Investigations) for further details.

42-2.9. Field offices and NCISRAs are highly encouraged to identify resources available in their area of responsibility that can provide training, assistance (manpower and logistics), media coverage, and legal and social services. Preplanning for the missing child investigation will prove to be very valuable in saving time and successfully managing these very demanding cases.

42-2.10. Missing Persons Review Board (MPRB). Once a missing person investigation has been initiated, the investigation cannot be closed for lack of investigative leads or inability to locate the victim. However, this may result in an investigation that languishes or indicates the possibility of the victim's death. Therefore, NCISHQ Code 23B has established the NCISHQ MPRB to examine investigations where a field office has determined all logical leads have been exhausted and the victim is still missing, or the victim may be deceased, but their remains cannot be found.

a. Requesting an NCISHQ MPRB. When a field office has determined that a missing person investigation has completed all logical leads, the case agent will send an ROI (ACTION) lead to the NCISHQ Code 23B DSI/SI (Missing Persons) desk officer to request an MPRB. The MPRB will be convened to examine the investigation and make a determination on the furtherance of the investigation. The MPRB can require the case remain open as a 7M (Missing Persons) or may refer the matter to SECNAV via the Navy Personnel Command (PERS-62) for an official death determination. Once SECNAV has issued an official determination, the MPRB can direct the case be changed to a 7H (Death) and fall within the current guidelines of the NCIS death investigations policy.

(1) Remain as Missing Person investigation. All missing person cases where the cause of the disappearance is unknown or possibly foul play is involved, are to remain in an open status. Once a missing person case has been thoroughly investigated and all logical leads have been exhausted, the MPRB will review the case and determine if any additional investigation is needed. If no further investigative efforts are necessary, the case will remain in an "open" status with the evidence and case file remaining at the control office. It will be incumbent upon the control office to conduct periodic inquiries (e.g., database checks, interviews, contact with local law enforcement) every 90 days to ascertain if there have been any new developments. These inquiries and attempts will be documented in an ROI (INTERIM). After one year, if no new information is developed, the case will be resubmitted to the MPRB. The MPRB will either direct the control office to continue the periodic inquiries or consideration will be given to have the project identifier changed to an NC or MC. If appropriate, a cold case agent will then be identified and the case will be reassigned for investigation.

(2) Changed to Death investigation. Those cases in which a thoroughly documented investigation dictates the missing person met their demise by murder, accident, or self-imposed means, after an official determination of death has been received from SECNAV, the MPRB will direct the case to be changed to a Death investigation (7H). In those cases where the remains are not recovered, the case agent should make every effort to obtain a death certificate prior to submission to NCISHQ for closure. Liaison between the case agent and the medical examiner or the member's command may facilitate this. All efforts to obtain a death certificate will be documented via an IA. Once the MPRB changes the Missing Persons (7M) to a Death (7H) investigation, and if additional investigative efforts are warranted or ongoing, an NCISHQ Code 23B Death Investigations desk officer will become the point of contact for the case agent. Once the investigation is complete, the case agent and their respective field office will treat the investigation as any other death investigation, subjecting it to either a Death Review Panel (DRP) or NCISHQ Death Review Board (DRB) prior to closure. See NCIS-3, Chapter 30 (Death Investigations) for further information.

b. The NCISHQ Code 23B MPRB will consist of the follow voting members:

(1) Code 23B Division Chief, Criminal Investigations;

(2) Code 23B SSA, Criminal Investigations;

(3) Code 23B SSA, Cold Case Investigations; and

(4) Other member(s) as necessary or appropriate.

42-3. ELEMENTS OF THE CRIME

42-3.1. General. When a military member is missing it could be a violation of either Article 86, UCMJ, Unauthorized Absence (UA), or the more serious violation of Article 85, UCMJ, Desertion. These offenses are "military offenses" and have no equivalents in civilian criminal codes. The missing military member may be the victim of a crime, and the appropriate statutes and their elements apply.

a. When a military dependent is missing, there is no offense, per se. The dependent may be the victim of a crime, and the appropriate statutes and their elements apply.

42-3.2. Essential Elements of Desertion. Any member of the armed forces who:

a. Leaves or remains absent without authority from his/her unit, organization, or place of duty with intent to remain away permanently;

b. Quits his/her unit, organization, or place of duty with intent to avoid hazardous duty or shirk important service; or

c. Enlists or accepts an appointment in one of the armed forces without fully disclosing the fact that he/she has not been regularly separated from the same or other armed forces division; or

d. Enters any foreign armed service, except when authorized by the United States; is guilty of desertion.

e. Any commissioned officer of the armed forces who, after tender of his/her resignation and before notice of its acceptance, quits his/her post or proper duties without leave and with the intent to remain away permanently is guilty of desertion.

2-3.3. Legal Discussion - Desertion. Under Article 85 of the UCMJ, there are four types of Desertion:

a. Desertion with Intent to Remain Away Permanently,

b. Desertion with Intent to Avoid Hazardous Duty or to Shirk Important Service,

c. Desertion Before Notice of Acceptance of Resignation, and

d. Attempted Desertion.

The intent to remain away permanently may be formed at any time during the unauthorized absence. The intent need not exist throughout the absence, or for any particular period of time, as long as it exists at some time during the absence. The intent to remain away permanently may be established by circumstantial evidence.

42-3.4. Legal Discussion - Absence Without Leave. This offense is referred to as “UA” (unauthorized absence) in the USN and USMC, and “AWOL” (absence without leave) in the Army and Air Force. Any member of the armed forces who, without authority, fails to go to his appointed place of duty at the time prescribed, or departs from that place, or absents himself from his unit, organization, or place of duty at which he is required to be at the time prescribed, shall be absent without leave.

a. Article 86 is designed to cover every other case not elsewhere provided for in the UCMJ when it is the armed forces member's own fault (e.g., changing muster location/time without notifying service member would not would not necessarily be the member's fault).

b. Failure to go to and leaving from appointed place of duty requires proof that the accused actually knew of the appointed time and place of duty. Actual knowledge may be proved circumstantially. Specific intent is not an element of unauthorized absence.

42-4. INVESTIGATIVE CONSIDERATIONS

(b)(7)(E)

Pages 1272 through 1279 redacted for the following reasons:
- -
(b)(7)(E)

NCIS-3, CHAPTER 43
CI SUPPORT TO RESEARCH, DEVELOPMENT AND ACQUISITION
EFFECTIVE DATE: AUGUST 2013

Table of Contents

REFERENCES

(a) SECNAVINST 5430.107 (28 Dec 2005) Mission and Functions of the Naval Criminal Investigative Service
(b) DoD Instruction 5200.39 (28 Dec 2010) Critical Program Information (CPI) Protection Within Department of Defense
(c) DoD Instruction O-5240.24 (08 Jun 2011) Counterintelligence (CI) Activities Supporting Research, Development and Acquisition (RDA)

49-1. Purpose. This chapter establishes and provides guidance for the NCIS Counterintelligence (CI) support to United States Navy (U.S. Navy) Research, Development and Acquisition (RDA) programs. Historically, NCIS has provided CI functional service support to U.S. Navy Research, Development, Testing and Evaluation (RDT&E) facilities and RDA programs. Because of the enormous financial investment in research and development, combined with the innovation of technology in our community, the Department of the Navy (DON) enjoys a strategic advantage over our potential adversaries. This, however, makes U.S. naval technology a primary intelligence collection target of foreign nations seeking to upgrade their own military capabilities. Successful foreign intelligence service (FIS) attempts to compromise U.S. technology result in significant reduction to the U.S. global military advantage and represent a continuing liability for future U.S. naval operations. Although over 100 countries currently conduct varying levels of intelligence activities against the DON, a relatively small number of

adversarial nation intelligence services constitute the primary intelligence threat. The loss of key technology either by deliberate theft or through carelessness or compromise endangers the lives of our service members and threatens our national security. This research may also be stolen, taken abroad, and incorporated into foreign products for sale to the U.S. market. NCIS RDA protection efforts must develop, evaluate and integrate CI support to the USN RDA programs to prevent the exploitation, destruction or compromise of identified critical technologies and information. NCIS RDA protection personnel must manage, integrate and promote programs that identify, counter, exploit, mitigate and neutralize FIS methods that target DON's defense research information, the supply chain, critical program information (CPI) and critical defense technology. This chapter is intended to help agents understand the processes that the DoD, DON, and NCIS have put into place to help ensure our technological edge.

43-2. Policy. References (a) through (c) are the primary DoD and Secretary of the Navy (SECNAV) instructions outlining and assigning responsibilities for RDA CI protection to NCIS. The guidelines set forth in these DoD instructions should be reviewed on a periodic basis by all personnel having RDA protection responsibilities to ensure that NCIS RDA services are aligned with DoD policy. NCIS is currently in the process of transitioning from a Defensive Research and Technology Protection process into a "Threat Based" program targeting the intelligence and technology gaps of our highest priority adversarial targets. From this process, major technology groups were identified as general technologies our adversaries are currently targeting. This list will be the focus of NCIS RDA protection efforts. This technology list allows maximum flexibility to move with the targets as they attempt to evade and elude our countering efforts and may change based on developing and emerging technologies and revalidation of the threat. The current list can be found on the NCIS SIPR website under the RDA tab.

43-3. Cancellation. None.

43-4. Sponsor. This chapter is sponsored by the NCIS National Security Directorate, Code 22C, RDA Program Office.

43-5. RDA Positions and Responsibilities. The National Security Directorate (NSD) is responsible for the overall strategic direction of the RDA program. Responsibilities include input into the budgeting cycle, policy development, staffing and training issues. Additionally, the NSD is responsible for issues regarding prioritization of NCIS coverage to DON RDT&E facilities, technology and acquisition programs. NSD will also validate the prioritized technology and program listing in relation to the current threat.

a. Research, Development and Acquisition Analyst at NCIS Headquarters and Field Level. Analytical support should first be coordinated with local NCIS field office analysts, where available. Field analysts, or agents when analysts are unavailable, will coordinate with the RDA Analytical Division to develop products to support investigations, XXRDs, XXTPs, and/or counterintelligence support plans (CISPs). The RDA Division located within the Directorate of Intelligence and Information Sharing (DIIS) is responsible to provide finished intelligence products to both the NCIS field offices and the DON System Commands (SYSCOM). RDA Analytical Division is made up of two groups of personnel. The first group works in the DoD Supply Chain Risk Management - Threat Analysis Center (SCRM/TAC) and provides analytical

support directly to DON acquisition community by producing analytical reports regarding threats posed to the DON supply chain. The second group is located with the rest of the DIIS analysts in the Multiple Threat Analysis Center (MTAC) and provides support to DON by producing analytical reports regarding threats posed to SYSCOM programs.

b. The RDA product line consists of:

(b)(7)(E)

(b)(7)(E)

d. SYSCOM CI Representatives. The SYSCOM CI representative is a special agent who supports the NCIS CI and RDA program at one of the Navy's four major acquisition SYSCOMs; Naval Sea Systems Command, Naval Air Systems Command, Space and Warfare Systems Command, and Marine Corp Systems Command. The SYSCOM CI representative is in a unique position of responsibility in a strategic location and plays a vital role in the overall execution of the RDA program. The SYSCOM CI representative is responsible for identifying significant and critical issues for the SYSCOM commander warranting CI support. The representative will be responsive to the needs of the SYSCOM. SYSCOM CI representatives must be aware and familiar with NCIS policies, methodologies, contacts, and strategies to guide and advise commands. The SYSCOM CI representative should attend command meetings and working groups, advising senior officers and civilians on probable courses of action or appropriate responses to emerging CI issues. SYSCOM CI Representative Responsibilities include:

(b)(7)(E)

Page 1284 redacted for the following reason:
- - - - - - - - - - - - - - - - - - - -
(b)(7)(E)

(b)(7)(E)

(b) Simultaneously, the NSD, with input from the CI representative, will prioritize and evaluate the level of CI support to be provided to the program.

e. Special Agent - Field Level, CI/Technology Protection. NCIS special agents providing CI support to RDA will focus on either an RDT&E facility or an RDA acquisition program or technology identified as a priority, which may or may not contain CPI. Special agents are responsible for providing or coordinating CI support, being the RDT&E facility or acquisition program manager's (PM's) NCIS point of contact, and keeping PMs briefed on all NCIS activities concerning the facility, acquisition program, or CPI receiving CI support. Travel to meet with program personnel and, or managers may be required occasionally. The NCIS special agent should evaluate whether he or she should be involved in numerous and lengthy non-CI investigations or operations as those activities will detract from the required support. Ideally, those investigations or operations should be referred to other NCIS special agents.

f. Sensitive Technologies. NCIS provides CI support to select sensitive naval technologies. Support to certain U.S. Navy equities requires special access and extensive coordination to ensure a seamless process for supported customers. All efforts in this area are handled by a select group of program briefed special agents. Any requirements in relation to sensitive U.S. Navy equities must be coordinated via classified communications through the NCIS Office of Strategic Support (OSS).

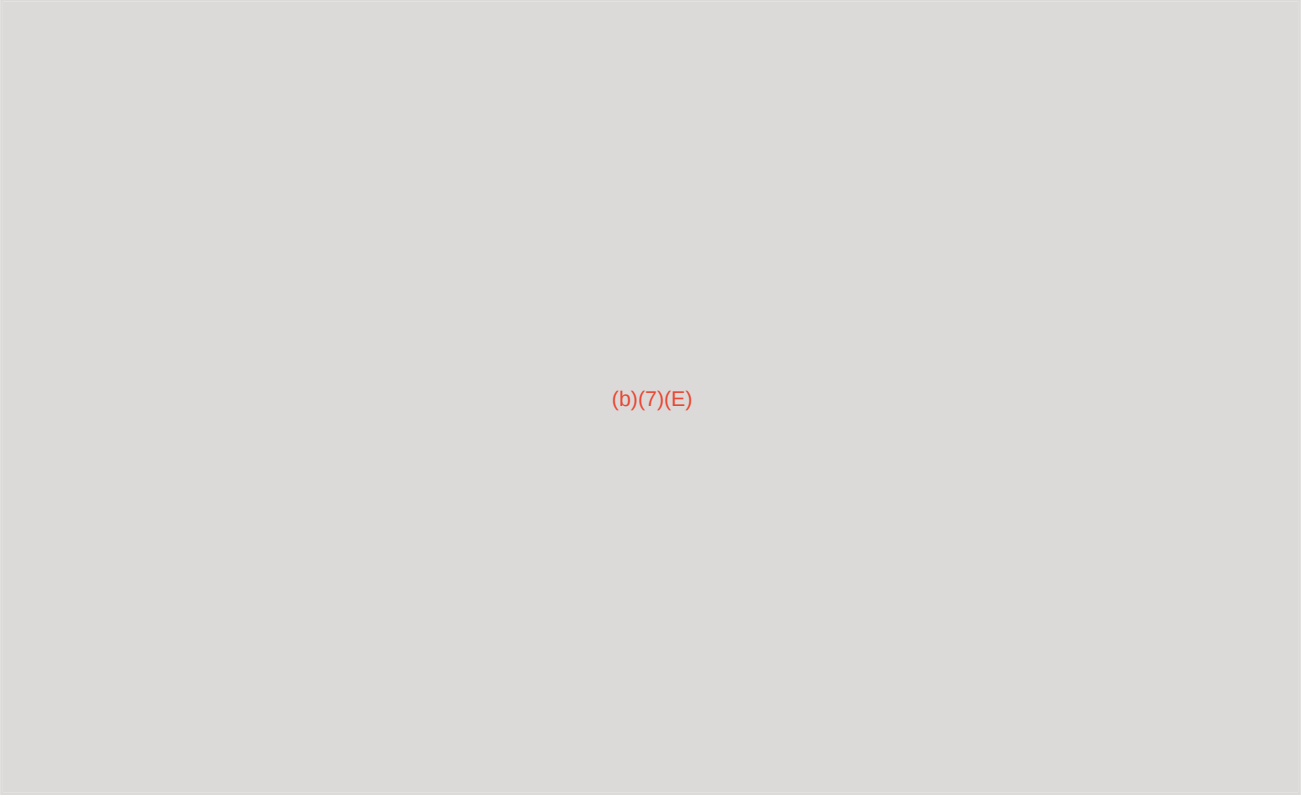
g. Naval Nuclear Propulsion Program (NNPP). Notification of the NNPP, sometimes referred to as Naval Reactors (NR), is required for all NCIS investigations involving or targeting DON personnel or programs associated with NNPP. NCIS has assigned a senior representative to NNPP who facilitates and coordinates between NCIS field elements and NNPP command leadership. Field notification to the NCIS NNPP senior representative must be submitted via the NCIS report writing system. All CI reports must include a lead to Code 22B requesting notification be made to the NCIS NNPP senior representative.

h. SLDCADA Codes. NCIS Special Agents providing CI Support to RDA must use the appropriate SLDCADA code (primarily FC-06, RDA Activities or FC-07, CI Activity in Support of Strategic Programs) to document time expended in support of RDA. This SLDCADA code must be used for all CI activities conducted supporting USN RDA programs, including briefings, travel briefings and debriefings, investigations, etc. Maintaining an accurate accounting of time spent supporting RDA is critical due to periodic audits conducted by the NCIS resource sponsors. NCIS is authorized funding specifically to support RDA activities and is required to demonstrate the corresponding level of effort.

43-6. Laying the Groundwork for a Successful RDA Program. NCIS special agents providing CI support to an RDT&E facility or acquisition program are responsible for providing or coordinating CI support, being the RDT&E Facility and or Program Manager's NCIS point of contact, and keep them briefed on all NCIS activities affecting the facility or its activities. The

following steps provide, in general terms, how to lay the groundwork for providing successful CI support to a facility or program:

a. These personnel include:



b. Identify and meet with key outside agency contacts.

(1) Defense Security Service (DSS). DSS administers the Industrial Security Program, conducts facility inspection reports on cleared defense contractors, maintains contact with cleared defense contractors, and reviews debriefing reports from contractor employees responsive to reportable situations.

(2) DSS Industrial Security (IS) Representatives. IS representatives coordinate support to cleared contractor facilities and universities with the local DSS representative and the DSS IS representative responsible for that RDT&E facility. Offer to help them on base with military offices and personnel that they need to visit. The DSS IS representative will need to facilitate initial interactions at contractor facilities and university locations.

(3) Federal Bureau of Investigation (FBI). Contact the local FBI office and request to be placed on their awareness of national security issues and response (ANSIR) e-mail. Other key FBI special agents include the Domain Coordinator located in each FBI field office.

(4) Bureau of Immigration and Customs Enforcement (ICE). ICE is the lead U.S. agency for investigating violations of International Traffic in Arms Regulation (ITAR). ICE can

provide details on current investigations and insight into unauthorized foreign technology transfer trends and methodologies.

(5) U.S. Department of Commerce (DOC) Office of Export Enforcement (OEE). DOC, OEE handles various export control issues. The DOC mission involves promoting U.S. competitiveness in the global marketplace by strengthening and safeguarding economic infrastructure with cutting-edge science and technology and an unrivaled information base.

(b)(7)(E)

43-7. RDA Operational Reporting. NCIS CI support efforts associated with RDT&E facilities and acquisition programs are documented via two distinct categories of operations, XXRD and XXTP (see below). The operations are designed to capture, in an overarching fashion, all investigative, information collection, lead generation, defensive activity and reporting related to the specific operation. Transmission of lead tasking/action leads to other NCIS offices are authorized under both of these documents. RDA designated agents are not required to initiate a separate collection operation (XXCC) when the facility or technology is covered by an active XXRD or XXTP operation (see section 43-12, Source Utilization for RDA). Specifically, the official NCIS case categories and definitions are:

a. Counterintelligence Support to RDT&E Facilities - (XXRD). This category documents CI support to RDT&E facilities. It may also include a Cleared Defense Contractor site that by nature of the DON technology being developed may warrant CI support. This operation does not require NSD Operational Review Board (ORB) approval, but does require close coordination with the NSD NCISHQ RDA desk officer. XXRD and XXTP ROI Interims are authorized and can be used to send and receive lead tasking.

b. Counterintelligence Support to Acquisition Programs - (XXTP). This category documents activities associated with CI support to a specific acquisition program, developing technology, or Defense Critical National Asset (CNA). The goal is for NCIS to support a particular technology acquisition program throughout its life cycle. Life cycle support takes it from its inception, through deployment, to demilitarization. This means that, as technology transitions, the NCIS unit responsible for CI support will change. NCIS Special Agents and managers should be aware of the special technologies they support and should contact and/or task NCIS offices when that particular technology is deploying to another NCIS field office AOR. It is very important that information be shared for deployed or fielded technologies, as well as those being displayed at air shows or other public events. This operation does not require NSD ORB process or approval but does require close coordination with the NSD desk officer. XXRD and XXTP ROI Interims are authorized and can be used to send and receive lead tasking.

(1) For U.S. Navy RDA programs or locations in which the CPI is present year round, the appropriate response would be to initiate a CI TECHNOLOGY PROTECTION SUPPORT (XXTP) Operation.

(2) The XXTP should remain continuously open so long as support is provided to a particular technology. For locations in which the CPI is present only intermittently, i.e. a testing location or range, the appropriate response is to report the support under the existing XXTP for the CPI.

c. Operational Proposal. The first document drafted by an agent should be the operational proposal. The operational proposal will be attached to the ROI (Open) as an exhibit and the NSD desk officer upon receipt will review the proposal. The following format should be used for this document:

(1) The operational proposal will not be reviewed and approved by the NSD ORB. Only offensive CI operations (i.e., Controlled Source Operations) require ORB process and approval.

(2) The following information should be provided for the XXRD or XXTP operational proposal;

(b)(7)(E)

(b)(7)(E)

e. The Counterintelligence Support Plan (CISP). After opening the operation or reviewing the existing operational file, an umbrella CISP or a tailored DoD CISP shall either be developed or updated. The CISP is a jointly developed document mandated for use by DoD and is a DoD Inspector General (DoDIG) or NCIS and Navy Inspector General item of interest. This document will be updated for signature by the command every three years, but will be reviewed with appropriate management on an annual basis. All signed CISPs will be attached as an exhibit and forwarded to NCIS headquarters for retention via a supporting XXRD or XXTP operation. For some locations or facilities, primarily for reasons of resource constraints, an umbrella CISP will detail CI support to a facility vice a specifically tailored, focused CISP. CI support plans are dynamic documents and must be modified continuously because the environment is elastic and the threat asymmetric. Support plans must be reassessed and updated periodically, and on an event driven basis. Success may hinge on treating each critical component as an individual entity and then tailoring the protection plan to that specific component.

(b)(7)(E)

(b)(7)(E)

(c) Section III is an acknowledgement regarding annual review and tri-annual updating of the agreement.

(d) The case agent and the field office SAC or SSA will sign as the NCIS signatory to this agreement. An appropriate command representative will sign for the facility. There is no requirement for NCISHQ to sign or approve these agreements.

f. CISP for DoD Acquisition Program. Like the CISP for RDT&E facilities, a new CISP format for DoD acquisition programs has been prepared and execution is now mandatory for NCIS field activities. A copy of the format is provided as Appendix (B) to this chapter.

(1) Section I provides information on the overall acquisition program requiring enhanced CI support. There are nineteen subsections. RDA special agents should ensure the document is both accurate and comprehensive. The subheadings described in Appendix (B) should be self-explanatory.

(2) Section II serves as an overview of CI support to be provided by the NCIS and the requirements imposed upon government officials overseeing the acquisition program in assisting with this support. RDA special agents must be thoroughly familiar with the contents of section II since it outlines the nature of the CI support to be provided.

(3) Section III ensures the ability of NCIS to interact with contractors possessing Critical Program Information (CPI). Contractors are often reluctant to cooperate with NCIS on matters of counterintelligence due to the financial burden placed on them regarding the time expended by their employees. This section requires the acquisition program management to ensure NCIS access to these contractors.

(4) Section IV is the acknowledgement of an annual review and tri-annual updating of the CISP. The agreement will be signed by the responsible RDA special agent, SSA or SAC and an acquisition program manager with the authority to provide the required support. There is no requirement for NCISHQ to sign or approve this agreement.

g. CI Support Plan Addendum (CISP(A)). The CISP (A) will be utilized for any DoD contractor, to include universities that work on CPI as part of a DoD acquisitions program. This addendum should also be utilized for any DoD contractor identified as being involved in critical research information and technology as identified by RDT&E personnel. If the facility is involved with classified information, the Defense Security Service (DSS) must be involved.

(b)(7)(E)

(b)(7)(E)

h. ROI (Interim) Reporting. An ROI (Interim) is required every 60 days subsequent to releasing the Open. An example of a ROI (Interim) is included as Appendix (C). The above described CISP should be an exhibit to the initial ROI (Interim). Report formatting and classification should be in accordance with current NCIS policy regarding CI reporting. However, because of the long term nature of XXRD/XXTP special operations, it is not necessary to list all previous ROI (Interims) in the Reference section of the 60-day reports. Instead, cite in the reference section only the most recent previously submitted ROI (Interim) in all active investigations, briefings (9V, 9Z, 9F), threat assessments (5G), IIRs, and operations related to the operation initiated or pending during the current reporting period. At the conclusion of the operation, the closing ROI will reference all interim ROI reports written during the pendency of the operation. Appendix (D) is a sample ROI (Closed).

(1) Each reference must be discussed or summarized within the narrative section of the ROI (Interim). The narrative reporting must provide sufficient detail to provide an understanding of the operational activities, briefings, or coordination with the facility/program which occurred during the reporting period. Investigative Actions (IA) should be prepared to

record significant developments, meetings, events or briefings. Narrative reporting must include a discussion of each cited exhibit. Examples of appropriate exhibits would be the CISP, range schedules, etc. The Narrative section of every ROI (Interim) will include a section on metrics. Metric reporting will be provided for both the current reporting period and for the fiscal year to date; this is in line with Code 14 performance data call schedules. Accurate metrics must be maintained to satisfy the RDA performance measure requirements for NCIS and other agencies.

(2) The following is the standardized metric table currently required for use by NCISHQ:

Fiscal Year CI Support Oct-Oct	**Current**	**Fiscal Year to Date**
A. CI Awareness Briefs (9Z)	0	0
B. Foreign Visitor Escort Briefs (9V)	0	0
C. Defensive Briefs (9F)	0	0
D. Sources Supporting Operations	0	0
List Source by component code and sequential number, i.e. NFNF-0000		
E. Source Operations Initiated	0	0
F. IIRs Produced	0	0
G. IIR Evaluations Received	0	0
H. ROI (Info) Reports Produced	0	0
I. Investigations Initiated (Cat 3/5)	0	0
J. EEE Funds Expended	0	0

(Note): NSD has noticed an increase in the use of the 5M (OPSEC Support) case category to capture RDA efforts. Although the 5M category is an authorized category, if the efforts are in support of RDA matters, the 5M and any reporting generated as a result of the 5M needs to be properly documented within the XXRD/XXTP operations. If the 5M has been initiated to provide long term support to Cleared Defense Contractors (CDCs), then an XXRD case category needs to be used vice the 5M case category to capture RDA efforts to CDCs.

43-8. CI Support Activities. Core CI activities: In the scenario section of an XXRD or XXTP proposal, outline the specific CI support activities envisioned as necessary to support a facility or program. As stated before, Agents should be familiar with DoD guidance as outlined in DoD reference (b). The core activities at a minimum should be addressed in both the proposal and the support provided to the command. Core CI activities are:

(b)(7)(E)

Pages 1294 through 1295 redacted for the following reasons:
- -
(b)(7)(E)

(b)(7)(E)

43-9. CI Threat Assessment. Multi-disciplinary CI threat assessment (Case Category 5G) As noted earlier during the discussion of reference (b), a requirement was set forth for NCIS to provide a counterintelligence threat assessment with regards to the protection of an acquisition program holding CPI. NCIS meets this requirement with an analytical product titled the Multi-Disciplinary Counterintelligence Threat Assessment (MDCITA).

(a) If locally supporting an acquisition program holding CPI, an MDCITA may have already been requested by the SYSCOM's assigned SCIO. If so, a copy of the current MDCITA should be obtained by the agent, reviewed for familiarity, and retained in the operational file. The assigned RDA agent should also make a copy available to the local program manager for review.

(b) To request a new MDCITA in support of a program with CPI, the assigned agent will initiate an ROI (Open), case category 5G, Request for Multi-Disciplinary Counter Intelligence Threat Assessment. Lead tasking requesting the MDCITA will be made to the MTAC RDA Division.

(c) The request for this threat assessment shall be on Command letterhead and accompanied by:

(1) Documents that identify specific CPI.

(2) An explanation of why the CPI is critical.

(3) Known CPI locations and points of contact at those locations.

(4) Details regarding foreign interest in the program, technology, and CPI.

(5) The extent of foreign participation in joint ventures or DEA.

(6) Information surrounding known foreign military sales involved with the program, technology, and CPI.

(7) Information regarding known horizontal use (across the U.S. Armed Services) of the platform, weapon, technology, or CPI.

(8) The program protection plan or like document.

(b)(7)(E)

Pages 1298 through 1299 redacted for the following reasons:
- -
(b)(7)(E)

(b)(7)(E)

43-11. Requests for Information (RFI). Civilian government employees, cleared defense contractors, and U.S. military members by the nature of their position may receive suspicious RFI. This could occur via mail, e-mail, while traveling overseas, at technology conferences and air shows or during foreign visitor visits.

a. The following should be considered suspicious factors regarding an RFI:

(1) The CDC does not normally conduct business with the foreign requester.

(2) The request originates from an embargoed country.

(3) The request is unsolicited or unwarranted.

(4) The individual making the request claims to represent an official government agency, but he or she has gone outside of channels to make the request.

(5) The initial request is directed at employees who do not know the sender and is not in the sales or marketing office.

(6) The requester is fishing for information.

(7) The requester represents a "third party" who is not identified.

(8) The requester is located in a country with a collection history directed at U.S. cleared defense industry.

(9) The requester seems to be "skirting controls," often masking his true intent by making several similar e-mailed RFIs from different addresses.

b. When a company or command reports such requests, an intelligence information report (IIR) should be considered and used to alert the entire community to foreign intelligence collection attempts. E-mailed RFIs are the Method of Operation (MO) commonly used to collect US technology. Industry is prudent to detect, assess, and manage risk when it reports suspicious contacts and by presumably not responding to suspicious requests. DSS and, by extension, the National Counterintelligence Executive (NCIX), emphasizes the importance and long-term value of timely reporting by the cleared defense industry.

Pages 1301 through 1327 redacted for the following reasons:
- -
(b)(7)(E)

NCIS-3, CHAPTER 45
CYBER INVESTIGATIONS AND OPERATIONS
EFFECTIVE DATE: AUGUST 2013

Table of Contents

References:

(a) SECNAVINST 5430.107, Mission and Functions of the Naval Criminal Investigative Service, December 28, 2005
(b) SECNAVINST 5239.3B, Department of the Navy Information Assurance Policy, June 17, 2009
(c) SECNAVINST 3052.2, Cyberspace Policy and Administration within the Department of the Navy, March 6, 2009
(d) SECNAVINST 5239.19, Department of the Navy Computer Network Incident Response and Reporting Requirements, March 18, 2008
(e) Department of Defense Directive 8570.01, Information Assurance Training, Certification, and Workforce Management, August 15, 2004
(f) DoDI S-5240.17, Counterintelligence Collection, January 12, 2009
(g) NCIS GEN ADMIN 11C-0009, NCIS Military Counterintelligence Collection (MCC) Operations, April 21, 2011
(h) DoDI S-5240.23, Counterintelligence (CI) Activities in Cyberspace, December 13, 2010

45-1. Purpose. This chapter establishes policy and responsibilities, requirements and standards for the conduct and management of Cyber investigations specifically identified below.

45-2. Policy. It is NCIS policy that cyber investigations be conducted in accordance with Department of Defense (DoD) and Department of Navy (DON) instructions as set forth in this chapter and references (a) through (h).

45-3. Cancellation. None.

45-4. Chapter Sponsor. NCIS National Security Directorate, Cyber Department (Code 22D).

45-5. Objective. The objective of this chapter is to provide guidance on the conduct of cyber related investigations and operations and to provide reporting, oversight and management requirements.

45-6. Definitions

a. Acquisition. Acquisition is the process of collecting evidence from a device using forensically sound techniques. Automated forensic tools, except in cases where alternative acquisition methods are necessary, handle this process.

b. Advanced Analysis. Advanced analysis is the use of specific techniques to gain a more comprehensive understanding of the evidence beyond the triage-level in support of an investigation. This includes, but not limited to, logical and physical acquisitions, advanced data carving, examination of evidence obtained from physical acquisitions, and the limited use of non-standard techniques necessary to examine emergent technology.

c. Computer Network Attack (CNA). Actions taken using computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

d. Computer Network Exploitation (CNE). Enabling operations and intelligence collection capabilities conducted using computer networks to gather data from target or adversary automated information systems or networks.

e. Cyberspace. A global domain within the information environment consisting of the interdependent network of IT infrastructures, including the Internet, telecommunications and satellite networks, computer systems, and embedded processors and controllers.

f. Defensive Cyberspace Operations (DCO). Actions taken to protect, monitor, analyze, detect and respond to unauthorized activity within information systems and computer networks. Also referred to as computer network defense (CND).

g. Dynamic Global Information Grid (GIG) Operations. The employment of cyber capabilities to enable and support military operations. Such operations include activities to operate and defend the GIG (also known as "network operations").

h. Examination. Examination is the detailed, documented analysis of evidence to determine relevance to an investigation and to shed light on the facts regarding the case. The term "examination" is often used to refer to the whole process, from acquisition to reporting.

i. Information Assurance (IA). Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and response capabilities.

j. Information Operations. The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities noted in reference (c) enclosure (1). These are designed to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own.

k. Logical acquisitions. Logical acquisition is the use of a forensic tool to collect only data visible to the file system of the device. This can include a large amount of useful data, including photos, text messages, e-mails, and potentially metadata such as geo-location records. Logical acquisition may not collect all available data.

l. Manual acquisitions. Manual acquisitions involve navigation of the mobile device to document data present within internal memory. This process is time consuming, normally a last resort method of extracting data, and requires detailed written and photographic documentation of all steps.

m. Network Operations (NETOPS). Activities conducted to operate and defend the GIG.

n. Offensive Cyberspace Operations. Comprised of CNA, CND, and related CNE enabling operations (such as operational preparation of the environment).

o. Physical acquisitions. Physical acquisition is the use of a forensic tool to collect all data present on the mobile device's internal storage, whether it is part of the file system or not. In addition to collecting the data accessible by a logical acquisition, physical acquisition can extract data such as deleted or hidden files and system files not visible to the file system. The common mobile forensic tools are only able to provide physical acquisition capabilities for a subset of device manufacturers and models.

p. Triage. Triage-level forensics is conducted to quickly identify information and determine the potential evidentiary relevance. Triage may include, but is not limited to, tasks such as logical acquisition of the device and initial viewing of evidence.

45-7. General Information. Per reference (a), NCIS is the DON's primary law enforcement (LE) and counterintelligence (CI) agency charged with conducting felony level related investigations. As such,

NCIS is responsible for conducting high-interest cyber related investigations for Navy and Marine Corps computers and networks. While these investigations have been pursued historically as criminal offenses, the national security implications associated with these types of cases should be considered. Cyber investigations also provide a means of collection and reporting in support of other areas such as threat assessments, CI, criminal and terrorism investigations.

45-8. Jurisdiction and Policy

a. Reference (b) states NCIS maintains investigative authority for criminal acts or espionage related to computer network security incidents, and coordinates information regarding such incidents with the law enforcement and CI communities. It specifically directs the Director, NCIS, to:

(1) Conduct all investigations regarding operations, proactive programs, and related analyses of cyber incidents and targeting involving DON IT assets.

(2) Collect, track, and report threats to DON IT assets and disseminate this information to other law enforcement agencies, DoD, DON, DON CIO, and other national agencies, as needed.

(3) Conduct cyber-related criminal investigations regarding root level intrusions, user level intrusions, denial of service, malicious logic incidents, and aforementioned-suspected incidents (described as categories 1, 2, 4, and 7 in reference (d) and as outlined in paragraphs 45-9 through 45-12 of this chapter). Provide recommendations based on analysis of forensics to the DON CIO for incorporation into potential IA and CND policy.

(4) Investigate fraud, waste, abuse, and other criminal violations involving DON IT.

(5) Maintain a staff skilled in the investigation of computer crime. The staff should be sufficient in size to handle multiple major incidents and respond to increasing demands of the DON.

b. Reference (c) directs the Director, NCIS to:

(1) Investigate terrorism, foreign intelligence, and major criminal offenses impacting the DON from inside, on, and beyond the DON cyberspace perimeter.

(2) Conduct proactive cyberspace counter-terrorism, CI, and criminal operation programs related to DON and related defense industrial base assets.

(3) Coordinate with the Assistant Secretary of the Navy for Research, Development and Acquisition (ASN (RDA)) to:

(a) Enhance LE and CI capabilities and solutions for the research, development, and acquisition efforts that support the DON cyberspace domain and

(b) Enable horizontal protection of DON critical program information, critical unclassified information, and the supply-chain process.

(4) Coordinate and deliver LE and CI cyberspace training to NETOPS and computer incident response teams to ensure responses are conducted in a manner that supports LE and CI pursuit and prosecution objectives;

(5) Establish information sharing programs between naval and other intelligence organizations to facilitate national and international collaboration on LE and CI related efforts involving naval cyberspace intelligence objectives; and

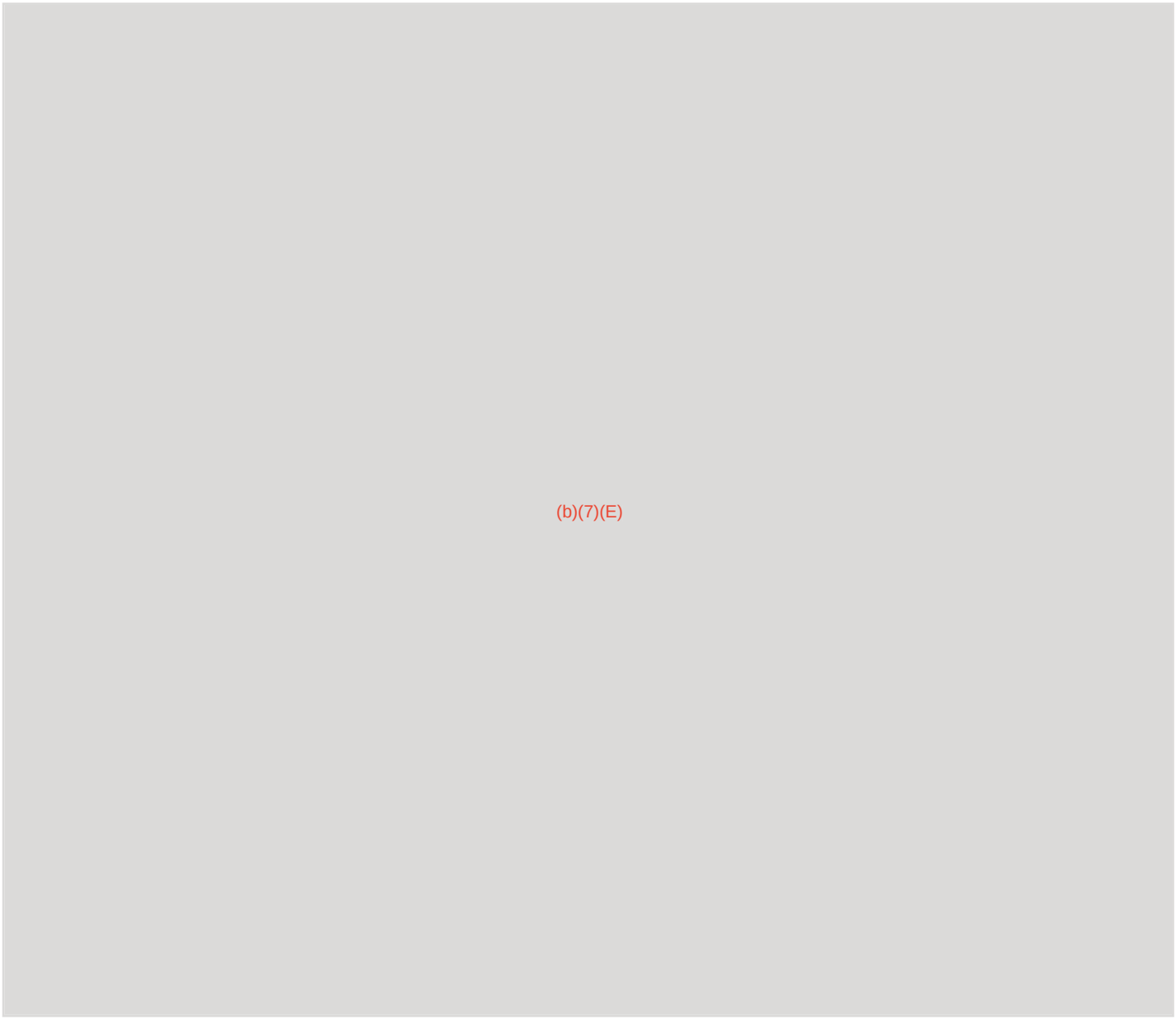
(6) Provide investigative and intelligence support for the Damage Assessment Management Office (DAMO) assessments to determine necessary follow-on actions.

c. Reference (d) requires all Navy and Marine Corps commands to report computer network attacks and intrusion incidents against Navy and Marine Corps systems. Commands must report to the respective Computer Network Defense Service Provider (CNDSP). For the Navy, the CNSDP is the Navy Cyber Defense Operations Command (NCDOC), Norfolk, Virginia and for the Marine Corps the CNDSP is the Marine Corps Network Operations and Security Center (MCNOSC), Quantico, Virginia. The CNDSPs are then required to report and coordinate any incident response with NCIS on all high interest computer network incidents. These high interest incidents are defined as root level intrusions, user level intrusions, denial of service attacks, and malicious code/events. NCIS is required to open investigations on all incidents that fall in these categories. It will be up to the Special Agent in Charge, Cyber Operations Field Office (CBFO), or their designee, to determine if a full investigation is warranted or if the incident can be documented via a ROI (Info). In the case of contractors, commercial entities, and private citizens providing support to the DON, NCIS will conduct proactive cyber activities when appropriate and feasible, particularly for threats from foreign intelligence entities and terrorists. NCIS is to provide the office of the DON Chief Information Officer (CIO) recommendations from its cyber forensic analysis obtained during its investigations and operations for incorporation into potential IA and network defense policy.

(b)(7)(E)

e. References (f), (g) and (h), are the primary DoD and NCIS instructions outlining and assigning responsibility for the conduct of counterintelligence collection and activities in a cyberspace environment. The guidelines set forth in these DoD and NCIS instructions should be reviewed on a periodic basis by all personnel having counterintelligence collection or operational responsibilities using cyberspace as a venue to ensure alignment with current policy.

Pages 1333 through 1334 redacted for the following reasons:
- -
(b)(7)(E)



45-9. Exceeding Authorized Access – Category 5H

a. Exceeding authorized access (5H), is defined by reference (d) (Category 2 - User Level Intrusion) as “unauthorized non-privileged access (user-develop permissions) to a DoD system. Automated tools, targeted exploits, or self-propagating malicious logic may also attain these privileges.” Category 5H involves a current or previous user who has or had legitimate access to the DON system in question. This user willfully uses their access and system knowledge to circumvent computer security protective measures to cause damage or steal proprietary data.

b. Insiders (witting or unwitting) represent the most significant threat to network systems since most security such as network intrusion prevention and detection systems are focused on external threats. An insider only has to elevate or exceed their authorized access or use their existing accesses for malicious

and destructive purposes. Insiders are likely to have specific goals and objectives in attacking an information system, and are able to determine the best method to attain their objective based on system knowledge. Insider attacks can affect all systems, and can do so with limited risk based on their knowledge of the system, organizational security practices, and plausible access requirements. Insider activities can range from browsing confidential files, to planting malicious code, to fraud. Browsing activities can disclose confidential personal information, such as medical records, corporate proprietary information, or sensitive government data. Insiders can also plant malicious code to gain attention, steal, or exact revenge. Insiders can affect system availability by overloading the system's processing or storage capacity, or by causing the system to crash. Additionally, the potential exists for substantial fraudulent activities, to include the diversion of money or property or the theft of valuable data, computer time, or telecommunications access.

c. Insider threat motivations vary, ranging from disgruntled employees, paid informants, compromised or coerced employees, or former employees. Motivators for this group include malicious intent, monetary gain, and revenge.

(1) Disgruntled employees believe their employer has treated them unfairly. This belief may result from believing they are underpaid, not respected by their peers or superiors, or unfairly treated in terms of promotion or advancement. A disgruntled system administrator has full access to the entire range of information within the organization's automated data system and has sufficient knowledge of the computer system to access data anonymously, bypassing audit and access control systems, or to covertly sabotage the system. Such individuals are primary targets for recruitment by foreign intelligence services, terrorists, criminal organizations, competitor intelligence organizations, and information brokers. Particular risk exists in the case of system administrators or other systems personnel who are terminated or quit under unfavorable circumstances. Personnel performing these duties can cause considerable damage and may be able to extract or transfer large amounts of data before their departure. Without appropriate safeguards, these individuals can place malware in the system that will not activate until after they have left. The employee can also destroy required back-up documentation, purposely insert erroneous data in the system, or misfile important information. Such employees must be denied access to supporting computer systems upon notification they are leaving or before notification of termination.

(2) Paid informants sell information to brokers, industrial spies, criminal organizations, and intelligence services. Information brokers have paid employees with legitimate access to provide data on unpublished telephone numbers, toll records, credit reports, and other personal data. They have also paid individuals to access U.S. Government systems.

(3) Compromised or coerced employees with access to sensitive data or computer systems containing sensitive information are high-value targets for compromise or coercion by criminal activities, terrorist organizations, foreign intelligence services, and industrial spies. Employees may be compromised by their activities or by family connections. They can be coerced through threats of harm to them or their families. Frequently, coercion attempts involve family members in another country who could be adversely affected by the group seeking information. The compromised or coerced employee, like any other insider, is likely to be successful in performing the assigned illegal functions.

(4) Former employees frequently retain the ability to access the information systems of their former organizations and extract data based on their knowledge of security countermeasures and system vulnerabilities. Former employees may have intimate knowledge of user name and password combinations, may retain access to the building, and may have the knowledge required to defeat callback mechanisms allowing them remote access. They often maintain personal relationships providing them a means to obtain information on security procedures, personnel, and organizational structures. They frequently keep manuals describing information system functions and lists of dial-in ports. In effect, the former employee can maintain all system privileges unless information system security managers ensure effective countermeasures are in place. Former employees may be motivated by a desire for revenge, monetary gain, or a combination of factors.

d. Damage potential from insider threats affects all DON information systems. The information handled by these systems is sought by a variety of intelligence, commercial, and criminal interests. Insiders willing to sell desirable information are likely to find a ready market. They can disable or disrupt communication or information management activities. A trusted insider familiar with security countermeasures and methods to defeat or counter them could undertake either activity. This process could also take place during the manufacturing of a computer or network element, or the development of complex software. In either case, the activity may remain undiscovered and would have a substantial probability of success. Potential threats from insiders must be considered when analyzing network vulnerabilities and developing risk assessments.

e. The establishment of a closely supervised personnel reliability program for high value systems may be required. Supervisors should be cognizant of their employee's personal situations and know when they are experiencing unusual stress. Particular attention should be paid to warning signs such as financial difficulties, emotional distress associated with a divorce or death, excessive gambling debts, and the suspicion of drug and alcohol abuse. Each of these events could be cause for denying access to information systems, temporarily suspending an employee's security clearance, and denying them access to classified information. Because of the elevated network privileges afforded system administrators, particular attention must be paid to the aforementioned warning signs for these employees. In an effort to improve security, organizations can implement a variety of security improvements:

(b)(7)(E)

(b)(7)(E)

45-10. Intrusions – Category 5I

a. Reference (d) defines intrusion (Category 1 – Root Level Intrusion) as "unauthorized privileged access (administrative or root access) to a DoD system." Automated tools, targeted exploits, or self-propagating malicious logic may also attain these privileges. Privileged access, often referred to as administrative or root access, provides unrestricted access to the system. This includes unauthorized access to information or account credentials that are used to perform administrative functions (e.g., domain administrator).

b. Category 5I involves the external threat, comprised of an individual gaining unauthorized access to a networked computer system normally by exploiting computer software. The exploited software could be comprised of the operating system or an application running on it. The perpetrator of this illegal intrusion, commonly referred to as a "hacker," could be a lone individual, a criminal group, a terrorist group, or an intelligence agent working for a nation state or terrorist organization. Regardless of who conducted the intrusion or computer trespass, the actor has committed a Federal criminal violation. NCIS investigates these intrusions with the intent of supporting a criminal prosecution. If the investigation produces evidence against either a foreign intelligence or terrorist group with no documented U.S. person or U.S. based person involvement, the criminal investigation will be closed and the matter can be pursued as a CI operation after consultation with NCISHQ Code 22B. Intelligence information reports (IIRs) should be published in the course of a CI operation to share adversary TTPs with the Intelligence Community (IC). These IIRs will be shared with key military and government cyber centers to include USCYBERCOM, C10F, MARFORCYBER, NCDOC, MCNOSC, DON CIO, and NCIJTF. Where practical, additional information related to the reported event will be provided upon request to help these commands understand the threat to the DoD and help them understand the adversary.

c. Hackers normally attempt to elevate their access level to the root or system administrator level to access all data on the network. The intruder may alter software programs causing performance problems or a total system crash. Information the hacker accesses is normally sensitive unclassified data and often contains personally identifiable data (PII). Theft of PII enables identity theft and financial fraud as well as intelligence targeting against DON personnel. These intrusions also endanger DON technology by enabling adversaries to replicate advanced capabilities without the associated research and development costs. The aggregation of sensitive unclassified information and data can elevate its sensitivity to a classified level, constituting a compromise of national security information.

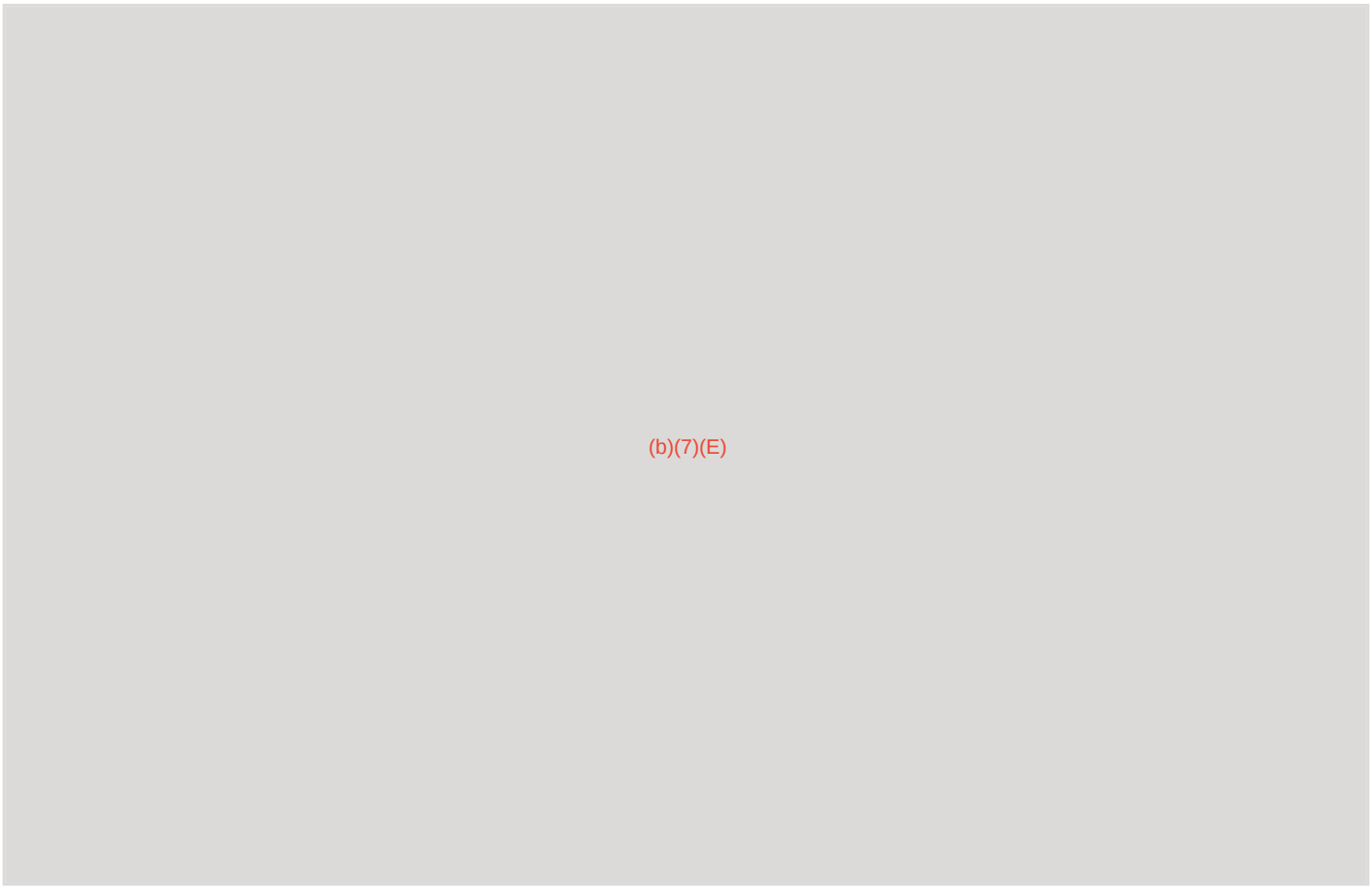
d. DON commands are to report all computer incidents directly to the appropriate DCO/CNDSP (NCDOC/MCNOSC). All high-interest security incidents (categories 1, 2, 4 & 7 per reference (d)) will be reported to NCIS for investigation. Appendix (A) is the NCIS incident response checklist for reference and guidance.

e. Intrusion activity often entails the removal or "exfiltration" of system or application files from the victim computer and delivery to the hacker's computer, often via command and control nodes or "hop points." These exfiltrated files are often encrypted. NCIS will attempt to decipher the files to determine the contents. Some files are exfiltrated without being encrypted. Examination of the victim computer may provide clues as to what was taken. Besides gaining clues about the hacker's TTPs, examination of the proprietary information that was exfiltrated may reveal intentions and, in some cases, provide indications and warnings of the adversary's follow-on actions. For example, the victim's e-mail contact list may reveal future targets for spear phishing e-mails. Files that are sensitive but unclassified (such as serialized documents, manuals, etc.) and reside inside web portals requiring PKI certifications or passwords are of special importance to the DON. State actors conduct intelligence-gathering operations on a massive scale against DoD networks to gain advantage over the U.S. in military design, tactics and technology. NCIS investigations of state sponsored intrusions should provide the warfighter with an understanding and impact of the stolen information so that designs, tactics, policies or procedures can be adjusted as required (a "battle damage" or "operational impact" assessment). Major intrusions and exfiltrations involving sensitive warfighter information should be reviewed by the Navy DAMO. Coordinate such a review with NSD Code 22D to work with DAMO officials. Other commands that may have an interest in exfiltrated DoD information include CYBERCOM, C10F, MARFORCYBER, Office of Naval Intelligence (ONI), US Marine Corps Intelligence Activity (MCIA) and the program executive officers of the Navy and Marine Corps system commands.

f. Legal provisions and considerations noted in paragraph 45-9 f. apply to intrusion and exfiltrations investigations.

45-11. Denial of Service – Category 5J

(b)(7)(E)



45-12. Malicious Code or Malware – Category 5K

a. Reference (d) defines malicious code or malware (Category 7 – Malicious Logic) as "installation of malicious software (e.g., Trojan, backdoor, virus, or worm)." Category 5K is used for investigations involving the installation of software designed and deployed by adversaries with malicious intentions for the purpose of gaining access to resources or information without the consent or knowledge of the user. This only includes malicious code that does not provide remote interactive control of the compromised system. Malicious code that has allowed interactive access is investigated under category 5I (Intrusion). Interactive access may include automated tools that establish an open channel of communications to and from a DoD system.

b. Viruses are software programs designed to spread from one file to another on a single computer. A virus might rapidly infect every application file on an individual computer, or slowly infect the documents, but it does not intentionally spread to other computers. Viruses can be either "benign" or "malignant." The majority of viruses are harmless and do not cause real damage to a computer or its files. A "benign" virus might do nothing more than display a message at a pre-determined time or slow down the performance of a computer. Malignant viruses damage a computer system by corrupting files or destroying data. These viruses wait for a predetermined date or set of circumstances before they are triggered to cause damage. Because a virus is classified malignant does not mean the damage it causes is intentional. A virus could be the result of poor programming or unintended bugs or mistakes in the software code.

c. Trojans are software programs which contain a hidden function intended by the programmer but unknown by the user. Sometimes this function creates a security breach allowing an unauthorized user system access, and other times this function can damage resident files on the system. Unlike viruses, Trojans do not multiply, but they can lead to both theft of proprietary data and destruction or alteration of resident files.

d. Worms are software programs which replicate themselves. However, instead of spreading from file to file, they spread from computer to computer until the entire network is infected.

e. Determining Malicious Code Thresholds. Before initiating an investigation, determine the severity of the code by assessing the rate of infection, the amount of damage, and the method of distribution.

(1) Rate of Infection. The rate at which malicious code spreads, or the wild component, measures the extent to which the code is replicating from computer to computer. Rate of infection classification guidelines: High (1,000 machines or 10 infected sites or multiple services or U.S. Government victimization); Medium (50-999 machines or 2 infected sites or multiple services or U.S. Government victimization); Low (anything else). Information in this metric includes:

(a) Number of independent sites infected.

(b) Number of computers infected.

(c) Geographic distribution of infection.

(d) Malware complexity (as defined by commercial anti-virus industry).

(2) Amount of Damage. Damage classification guidelines: High (file destruction or modification, very high server traffic, large-scale non-repairable damage, large security breaches, destructive triggers); Medium (non-critical settings altered, buggy software routines, easily repairable damage, non-destructive triggers); Low (no intentionally destructive behavior). Information in this metric includes:

(a) Triggered events.

(b) Clogged e-mail servers.

(c) Deleted or modified files.

(d) Release of sensitive, operational or classified information.

(e) System performance degradation.

(f) Poorly written software containing “bugs” that cause unintended loss of productivity.

(g) Compromised security settings.

(h) Level of effort needed to fix damage and restore system performance.

(3) Method of Distribution. Distribution classification guidelines: High (worms, network capable executables, uncontainable threats due to high virus complexity or low anti-virus ability to combat); Medium (most viruses); Low (most Trojans). This metric focuses on the method of distribution of the malicious code considering some of these possibilities:

(a) Large-scale e-mail attack (worm).

(b) Executable code attack (virus).

(c) Spreads only through download or copy (Trojan).

(d) Network drive infection capability.

(e) Difficulty to remove or repair.

(4) Threshold category. The overall severity measure unifies the three components above into a measure of risk to computer users and networks. There are five severity threat categories noted below:

(a) Category 5 (Very Severe). Highly dangerous threat type, very difficult to contain. All three components must be high (infection rate, amount of damage, and method of distribution).

(b) Category 4 (Severe). Dangerous threat type, difficult to contain. Two of the three components must be high (infection rate, amount of damage or method of distribution).

(c) Category 3 (Moderate). Threat characterized either as highly wild (but reasonably harmless and containable) or potentially dangerous (and uncontainable if released in the wild). Two of the three components must be high (infection rate, amount of damage or method of distribution).

(d) Category 2 (Small). Threat characterized either as low or moderately wild (but reasonably harmless and containable) or non-wild threat characterized by an unusually damaging or easily spreadable, or perhaps by some features of the virus that makes headlines. The infection rate component must be either low or moderate and the amount of damage or method of distribution components must be high).

(e) Category 1 (Minimal). Poses little threat to users or networks and there are no reports indicating the virus in the wild. All three components are Low.

f. Malicious code threats are significant. In accordance with reference (d), NCIS investigates those incidents affecting critical DON networks, warfighting capabilities, or threats to life or limb. Investigations will follow all logical leads to identify and support the prosecution of the perpetrator and document possible foreign intelligence or terrorist activity by publishing IIRs and possibly other analytical products.

g. Category 5K investigations will require close coordination with NCDOC and MCNOSC and could be conducted jointly with other law enforcement or CI authorities. The following details will be documented within ROIs: Malware name and version (if known), the type of malware (virus, worm, Trojan), properties of the malware (boot, file, macro, polymorphic), source of malware, infection vector (phishing e-mail, downloaded file, Website), the extent of the infection, initial impact to command and damage to network, loss value, and extradition issues related to perpetrators from outside the U.S. Databases from Code 22D, the NCIJTF, and USCYBERCOM will be queried and results documented for relevant data such as related cases of malware infections, sources of origin, and other such items designed to assist with the resolution and sharing of cyber related threat data. These queries will be coordinated with the 22D desk officer, and the NCIS representatives at the Defense Cyber Investigations Coordination Center (USCYBERCOM J3 LE entity) and the NCIJTF. These NCIS representatives will conduct appropriate database queries and collaborate with effected agencies at their locations.

45-13. Mobile Device Handling, Acquisition, and Reporting Procedures. Mobile phones and other personal handheld mobile devices are commonplace in today's society, and are widely used for both personal and professional purposes. These devices include but are not limited to, cellular phones, personal data assistants, computer tablets, personal navigation devices, global positioning system devices, audio video and photographic recording devices and all accompanying removable digital media. For investigators, these highly personalized mobile devices have become an increasingly routine item for the recovery of digital evidence. However, recovering data from these devices relevant to an investigation can pose a challenge requiring guidance. The information contained herein provides assistance regarding that forensic process.

a. Capabilities and Responsibilities

(1) The task of conducting forensics on mobile devices is the responsibility of three groups within NCIS: Cyber Operations Field Office, Technical Services Division, and trained geographic field office personnel. All three groups have the capability to conduct triage-level forensics. Certain personnel within the cyber and technical service disciplines have advanced training, and are able to conduct comprehensive forensic analysis.

(2) Initial attempts to conduct data extractions should be conducted by trained geographic field office personnel who have access to the proper mobile device forensic equipment. If proper equipment is not available or the data extractions are not conducted successfully, support should be requested from local Cyber Operations Field Office or technical service elements. Headquarters elements of both cyber and technical services maintain a surge capacity to conduct media forensics in the event field resources cannot meet the requirement.

b. Required Training

(1) All NCIS personnel conducting forensic examinations of mobile devices shall have appropriate training on the tools used to conduct the examination. The training required depends on the scope and depth of the forensic examination.

(2) The minimum level of training for NCIS personnel conducting acquisitions of mobile devices is attendance at an NCISHQ approved standard training session. The training session shall cover the essential functions of the tool, procedures to ensure the preservation of evidence, and reporting requirements. Following the classroom training, completion of a practical exercise is required to confirm their ability to extract data from mobile devices.

(3) Personnel conducting advanced analysis, including analysis of physical images, shall have training provided at the Federal Law Enforcement Training Center (FLETC), Glynco, Georgia, the Defense Cyber Investigations Training Academy (DCITA), Linthicum, Maryland, or attendance at vendor training.

c. Legal Considerations

(1) Permissive authorization for search and seizure and search warrants for data extraction from mobile devices.

(a) A permissive authorization for search and seizure (PASS) is one method by which to obtain access to the mobile media device. This method should always be documented as required by NCIS-3, Chapter 17 and should be executed as soon as the authorization is provided. The following language should be used for the PASS to allow all participants in the process to have access to the device:

1. This search and seizure may be conducted on DDMONYR and subsequent days as necessary to complete the computer forensic examination of all electronic storage media found during the search by Special Agent (insert name) and all other law enforcement forensic personnel as may be necessary. I hereby give these law enforcement personnel my permission to copy and retain any information found during the search, which is desired for investigative purposes.

2. I also give permission to NCIS special agents and other law enforcement personnel to conduct forensic reviews, by persons qualified to conduct said examinations, of all electronic storage media and data files, to include text and graphical image files, contained on the electronic storage media attached to or accompanying the described seized equipment (such as but not limited to computers and other devices) for investigative purposes pursuant to the investigation listed above.

(b) The consenting party may revoke a PASS at any time. If consent is revoked, and probable cause does not exist to obtain a search warrant, the device must be returned to the owner, losing an opportunity to obtain additional information. Any copies made before consent was revoked may be kept and analyzed at any time.

(c) When a PASS is not granted or obtained, and probable cause exists that the contents of the mobile device contain items of evidentiary value, an affidavit requesting authorization for search must be prepared by a special agent. This affidavit should be presented to the appropriate judicial authority from which a search warrant is requested. As a matter of practice, the use of search warrants or command authorized searches is preferred to a pass whenever probable cause exists. Procedures noted in NCIS-3, Chapter 17 for execution of the search warrant and return of the warrant to the authorizing judicial official must be followed.

Pages 1345 through 1346 redacted for the following reasons:
- -
(b)(7)(E)

the body of the external casing, and may appear in the interior of the battery compartment. However, do not remove the battery to read this information until the device has been properly powered off.

h. Examination and Acquisition

(1) Logical vs. Physical Acquisitions. For the purposes of a triage-level examination, only the logical acquisition is expected. It will often be sufficient for triage-level needs and is much quicker to execute. If time and the capability of available tools permits, a physical image may be collected concurrently with the logical image for use in later advanced analysis. Due to the more thorough and forensically sound nature of physical images, their use is preferred for conducting advanced analysis.

(2) General action steps. The detailed steps and procedures to be taken in technically performing a forensic acquisition of a mobile device are covered in training, vendor documentation, and any applicable field manuals. Regardless of the device or skill level of the examiner, the following steps must be performed at the beginning of the process.

(b)(7)(E)

(f) Complete the Mobile Device Investigations Worksheet (Appendix B). This worksheet should be maintained as a log with the examination device, i.e. *Cellebrite* mobile forensics and data extraction hardware.

i. Documenting the Examination

(1) Examiners will create a comprehensive electronic file to record information pertaining to each forensic examination. The examination report documents the examiner's inspection methodology, forensic process and findings. At the conclusion of the examination, the examiner will have created a comprehensive electronic file containing acquired images, examiner notes, research, and tool extraction reports. Figure 1 depicts a sample structure of these folders.

(2) The case control number (CCN) folder is the overall case folder, which contains all the sub-folders relevant to the examination. This folder should be named with the CCN, but the name can also

include an evidence log number hyphenated at the end of the CCN.

(3) The Case Photographs folder can be used to store photographs taken of the device by the examiner. The photographs document the condition of the phone when the examiner received it.

(4) The Case Notes folder is used to store notes taken by the examiner. If an examiner hand-writes notes, they may be scanned and saved into the folder. Scanned and electronic notes should be saved directly into the appropriate folder in a PDF document to prevent modification. Once complete, notes should be printed and a hard copy retained. At a minimum, these notes must include the date and time of all forensic action taken, the action performed and results (e.g. success and failure, information obtained) of that action. Any actions taken which constitute a change to the device, such as putting it in airplane mode, connecting a USB device or automatic upload of software by a forensic tool must be specifically documented in examiner notes. An example notes template is located in Appendix C.

(5) The Research folder can be used to store the device's user manual or any Internet research conducted regarding device parameters. Website research can be captured using tools like TechSmith and SnagIt, with the resultant captures being saved as a PDF file. The information collected may become useful if the device needs to be re-examined, or forwarded to a lab for a more in-depth examination. At a minimum, the examiner should download and save the device's user manual as questions about a device's capabilities may arise.

(6) The Tools folder is used to store all reports created by any of the acquisition or extraction tools used during the examination. If the tool has the ability to conduct both logical and physical acquisitions of a device, the examiner should create separate sub-folders for each type of report under the type of tool used.

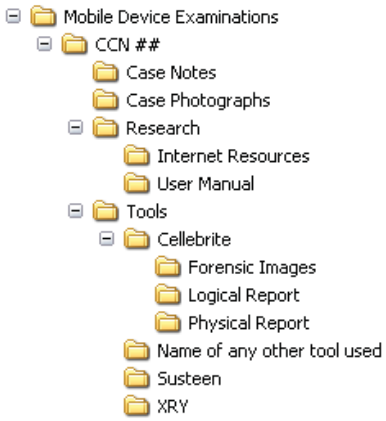


Figure 1: Sample Evidence File Structure

(7) The entire examiner-created file structure will be archived to one or more optical media. A hard drive may be used if acquiring a larger device or if the case results package is so large it cannot be easily broken down into smaller parts. It is recommended four copies of the file structure be copied to separate media. The first copy should serve as the evidence copy. The second copy should be the enclosure to the investigative action (IA). The third copy should be included in the examiner's lead case file notes

and the final copy should be provided to the case agent, investigator, or prosecutor as a working copy.

(8) The final step in documenting the examination is writing the IA. The IA should spell out the purpose and focus of the examination (e.g. the purpose of the search was to locate child pornographic images, or locate incriminating text messages or telephone numbers). The IA should also identify what legal authority the examiner has to examine the device (e.g. the device was examined under the permissive authority provided by the owner of the device). An example IA can be found in Appendix D.

45-14. Cyber Investigation Reporting Requirements

(b)(7)(E)

Pages 1350 through 1351 redacted for the following reasons:
- -
(b)(7)(E)

(k) The designated official will ensure the following information is sent to the DON CIO Privacy Office as soon as available, but no later than 30 days after discovery of the loss or suspected loss of PII: remedial actions taken to prevent reoccurrence; individual notification status, if notifications were required; lessons learned, if available; and disciplinary action taken, where appropriate.

45-15. Cyber Operations Reporting Requirements

a. NCIS cyber operational efforts are documented via its own distinct category of operations, Infrastructure Protection Operations (XXIP). This category documents cyber technical activities that do not involve direct source tasking, offensive CI operations or activities determined by the Special Agent in Charge (SAC) Cyber Operations Field Office (CBFO) or Division Chief, NSD Cyber Department to require Executive Level approval. These operations do not require NSD Operational Review Board (ORB) process or approval, but require close coordination with the NSD cyber desk officer and approval by NCIS NSD Attorney and SAC CBFO.

b. Operational Proposal. The first document drafted should be the operational proposal. The operational proposal will be attached to the ROI (Open) as an exhibit. The following format should be used for this document:

(1) Background. Reason for opening operation.

(2) Scenario. How this operation will be executed. This portion should include all technical details. Technical information should be extremely detailed and include all equipment, configurations, and software/hardware to be utilized and how they will be implemented. Technical schematics may be included as an attachment to the operational proposal.

(3) Objectives. What is expected to be achieved by conducting this operation? When applicable, what collection requirements will be addressed?

(4) Target. Threats to Department of Navy assets, if known.

(5) Funding Requirements. Description of funding required for hardware/software purchases, maintenance or travel.

(6) Manpower and Equipment. Requirements should be detailed and lay out the reasons these particular hardware, software and/or manpower solutions must be utilized. Justification will be required when cheaper solutions are available but not being implemented in support of the operation.

(7) Legal Considerations. Has a legal review been conducted of the scenario to ensure activities are operating within current laws and guidelines?

(8) Coordination. What command members or other agencies have been briefed and support this operational proposal? What support may they provide to assist in obtaining objectives?

c. ROI (Interim) Reporting. An ROI (Interim) is required every 60 days subsequent to releasing the Open. The report should include an Executive Summary providing a short, high level overview of the operation. The summary should provide sufficient detail of operational activities that have occurred during the reporting period. Investigative Actions (IA's) should be prepared to record significant developments. Narrative reporting must include a discussion of each cited exhibit. The narrative section of every ROI (Interim) will include a section on metrics. Metric reporting will be provided for both the current reporting period and for fiscal year to fiscal year. Accurate measurements must be maintained to satisfy the Cyber performance requirements for NCIS and other agencies.

The following is the standardized metric table currently required for use by NCISHQ:

Fiscal Year Cyber Support OctXX to OctXX	Current	Fiscal Year to Date
A. CSO Operations Initiated	0	0
B. IIRs Produced	0	0
C. IIR Evaluations Received	0	0
D. ROI (Info) Reports Produced	0	0
E. Investigations Initiated (Cat 3/5)	0	0
F. Operations Initiated (Cat 3/5)	0	0
G. Sources	0	0
H. EEE Funds Expended	0	0

45-16. Training Requirements

(b)(7)(E)

(b)(7)(E)

c. Additional Training. Continuing education is required for the maintenance of the CCCI and CDFE as well as to ensure the cyber workforce remains current in cyber investigations and emerging technology. Specific training requirements evolve with technology and will be defined by NSD Cyber.

Pages 1355 through 1366 redacted for the following reasons:
- -
(b)(7)(E)

NCIS-3, Chapter 46
Intelligence and Information Sharing Directorate
Department of Defense Law Enforcement Defense Data Exchange (D-DEx)
Effective Date: February 2015

TABLE OF CONTENTS **PAGE**

Current Policy Gen Admin:
(a) Gen Admin 23-0010, LInX Program Update and Use in the Field, 21 March 2008

References:
(a) DoD Instruction 5525.16, Law Enforcement Defense Data Exchange (LE D-DEx), 29 August 2013
(b) DoD Directive 5124.02, Under Secretary of Defense for Personnel and Readiness (USD(P&R)), 23 June 2008
(c) Secretary of Defense Correspondence Action Report, Lead for Integrating DoD Crime Databases into a Federal System, 2 August 2005

46-1. Purpose. This chapter defines the use, rules, responsibilities, reporting methods for NCIS users of the Department of Defense (DoD) Law Enforcement Defense Data Exchange (D-DEx) and other partner systems for automated law enforcement information sharing, such as the Law Enforcement Information Exchange (LInX) and the National Data Exchange (N-DEx), in accordance with references (a), (b), and (c).

46-2. Policy. NCIS promotes and enables information sharing with local, state, and Federal law enforcement partners of interest by facilitating the rapid, automated sharing of existing law enforcement data through the LInX and D-DEx database systems. The use of D-DEx is permissible for all case categories in which criminal activity is suspected. However, it is not to be used as a mass screening tool. See Appendix A for obtaining access and Appendix B for rules of use.

46-3. Cancellation. Gen Admin 23-0010, LInX Program Update and Use in the Field, 21 March 2008.

46-4. Chapter sponsor. Directorate of Intelligence and Information Sharing (DIIS), Code 25, D-DEx Division.

46-5. LInX, D-DEx, and Other Information Sharing Systems

a. The Law Enforcement Information Exchange (LInX). LInX was developed by NCIS and became operational in 2003. The goal was to provide automated, rapid sharing of law enforcement data already in the records management systems (RMSs) of law enforcement agencies in regions of the country of particular interest to the DON and NCIS. The primary purposes of LInX are to rapidly identify suspects, generate leads to solve crimes and prevent terrorism, resolve suspicious incidents, and provide context to those incidents. Although NCIS provides substantial funding for the LInX system, each LInX region is governed by its own board of governance (BOG), which includes the heads of each participating agency. The National LInX Regions BOG is made up of the chairs and co-chairs of each regional BOG. Generally, each agency is required to share data in order to participate in LInX; however, an agency may restrict certain types of data, such as internal affairs investigations. Each agency retains control over its data, and each BOG decides which types of information will be shared. LInX, itself, is not a system of record; it is a replication of an agency's RMS data that is stored on separate and secure LInX servers known as a data warehouse.

b. LInX regions. Regional organizations are dynamic, and the list of participants is subject to change. At this time, LInX is operational in the following regions.

(1) Northwest (NW LInX) covers Alaska, Oregon, Washington, and parts of Idaho.

(2) California (CA LInX) primarily covers Southern California.

(3) Hawaii (HI LInX) covers the State of Hawaii.

(4) Rio Grande (RG LInX) covers New Mexico and west Texas.

(5) Gulf Coast (GC LInX) covers south Texas.

(6) Southeast (SE LInX) covers Georgia and Florida.

(7) Carolinas (NC LInX) covers North and South Carolina.

(8) Virginia (VA LInX) covers Virginia (excluding the National Capital Region).

(9) National Capital Region (NCR LInX) covers Washington, D.C., Maryland, and northern Virginia.

(10) Northeast (NE LInX) includes agencies in Connecticut.

c. Department of Defense Law Enforcement Defense Data Exchange (D-DEx). Building on the success of LInX, the Department of Defense determined it would be beneficial to develop a similar DoD-wide system known as Department of Defense Law Enforcement Defense Data Exchange, or D-DEx. Like the LInX system, D-DEx replicates data and stores it on a separate, secure server. When fully implemented, D-DEx will contain data from all of the DoD law

enforcement agencies. The D-DEx system may contain information that participating DoD agencies elect not to share outside of the DoD.

d. Partner systems. D-DEx is connected to the 10 LInX geographical regions and to the National Law Enforcement Data Exchange (N-DEx), which is administered by the Department of Justice and various private and regional systems. N-DEx may be queried from within D-DEx by selecting the appropriate "neighborhood(s)" or through direct access from an N-DEx portal in D-DEx. Searching such partner systems is encouraged, as they cover parts of the United States that are not covered in the LInX regions. Users should be aware that other systems may have different data sets and the data may be displayed differently.

46-6. Responsibilities

a. National LInX Regions BOG. Membership consists of LInX and D-DEx chairs and co-chairs.

b. Regional BOGs. Membership consists of the heads of each participating agency within the region.

c. D-DEx Regional Program Manager (RPM). Each NCIS field office and Headquarters directorate has an assigned RPM responsible for the following:

(1) Opening new accounts, ensuring users complete basic training before accessing the system, providing additional user training, and certifying D-DEx trainers.

(2) Approving case blocking and consulting to determine whether cases should be blocked.

(3) Conducting annual field office audits with the assistance of field office personnel and with the concurrence of the Special Agent in Charge.

(4) Being a subject matter expert. Providing information about prohibited D-DEx inquiries, such as certain types of background investigations, and collecting feedback to improve the system.

d. D-DEx trainer. Once certified by an RPM, the trainer is allowed to instruct others and is responsible for documenting the training in the system.

e. Authorized users. Users are responsible for utilizing the system for lawful purposes only and within all applicable regulations.

46-7. NCIS reports and D-DEx. NCIS data is shared with D-DEx from CLEOC (Consolidated Law Enforcement Operations Center). Data should be shared in D-DEx to the maximum extent consistent with existing rules and best business practices. Mugshots and FBI numbers are

attached to a CLEOC file after submission of booking information via the biometrics capture device, currently LiveScan.

a. Unclassified information. Only unclassified information is allowed in D-DEx. Classified information should NEVER be entered into the unclassified CLEOC system.

b. NCIS case categories excluded from D-DEx. Certain NCIS case categories are filtered out of D-DEx, even though they may be allowed in CLEOC:

(1) Security inquires. All category 1 cases.

(2) Background/Internal investigations. All category 2 cases.

(3) Espionage. All category 3 cases.

(4) CI/CT. All category 5 cases.

(5) Protection/Briefings/Tech/PG. All category 9 cases.

(6) Defensive ops. All category XX cases.

(7) Criminal operations. Project codes of SO and UO are blocked from D-DEx

c. Blocking cases. Cases that need to be blocked from D-DEx for extended periods or permanently should be communicated by a supervisor to the D-DEx Division at NCIS headquarters or to the D-DEx RPM assigned to the field office. This process requires the CCN, the reason it is being blocked, the name and title of the supervisor authorizing the block, and the future date at which the block may be re-evaluated.

(1) Routine blocking. The CLEOC application contains a function to block a case while it is in an open status. The case agent must use the blocking features in CLEOC, which includes identifying the supervisor who approved the blocking and the date that the blocking decision will be reviewed to see if the block is still appropriate.

(2) Routine blocking example. An example of a reason to block a case is when a law enforcement official is a suspect and the investigation could be endangered by exposing the information in D-DEx.

(3) Reviews. Blocked cases will be reviewed by the D-DEx Division at least once a year.

(4) Questions and assistance about blocking cases. Users with questions about whether to block a case should discuss it with their chain of command. RPMs are available for consultation.

APPENDIX A
OBTAINING ACCESS

1. Accounts. A Department of Defense Law Enforcement Defense Data Exchange (D-DEx) account provides access to both the D-DEx and the Law Enforcement Information Exchange (LInX) systems. Separate LInX accounts are unnecessary for most NCIS personnel. Each field office and Headquarters directorate has an assigned D-DEx Regional Program Manager (RPM). To request an account, contact your assigned RPM or the LInX/D-DEx Division at (b)(6), (b)(7)(C) (b)(6), (b)(7)(C) ncis.navy.mil.

(b)(7)(E)

5. Use. D-DEx should be accessed through a government or other authorized computer.

6. Feedback. The D-DEx interface includes a feedback function. It should be used to report success stories, give functionality feedback, and suggest new features that would be helpful to investigations. Urgent issues may be provided to the D-DEx Division directly through (b)(6), (b)(7)(C) (b)(6), (b)(7)(C) ncis.navy.mil or your D-DEx/LInX RPM.

APPENDIX B
RULES OF USE

1. D-DEx is to be used to thoroughly research relevant information on all NCIS investigations and operations in which criminal activity is suspected. However, it is not to be used as a mass screening tool. The best practice is for the case agent to conduct the D-DEx inquiry, as the case agent is most familiar with the case and most likely to identify pertinent results.

a. Allowed users. Support personnel and assigned analysts may conduct D-DEx inquiries. Watch standers in the Multiple Threat Alert Center may access D-DEx for a field user in urgent circumstances.

b. Periodic inquiries. In addition to the initial D-DEx inquiry conducted when the investigation is opened, periodic D-DEx inquiries should be conducted as additional information is developed.

c. Agent safety. In addition to investigative support, D-DEx is a primary tool for agent safety. NCIS users are encouraged to use the "watch list" function in D-DEx on active NCIS subjects so that the case agent will be alerted if the subject has a new contact with law enforcement. This function is managed under the "My D-DEx" section of the home page.

2. Validation. Data derived from D-DEx/LInX may be used for the primary purposes of rapid identification of suspects, assistance with suspicious incidents, and lead generation to solve crimes. However, any law enforcement action must be based on validated, approved data from the originating agency.

a. Use of NCIS data. The use of NCIS data in D-DEx by NCIS users is permissible in all ways that the same information is used now without further authorization.

b. Prohibited use of data. No D-DEx information derived from other agencies, including analytical products, may be used as a basis for action or disseminated outside of the D-DEx program for any purpose or in any other manner unless the person making the inquiry first obtains the express permission of the agency or agencies that contributed the information.

(1) The inclusion of D-DEx/LInX information in an official case file and any use of such information in the preparation of judicial process, such as affidavits, warrants, or subpoenas without prior permission of the contributing agency is prohibited. See section 5, below, for reporting procedures.

(2) The person making the D-DEx inquiry should contact the contributing agency to determine whether the information is current, correct, and complete, and to request a copy of the actual report for inclusion in the NCIS case file.

(3) Various memoranda of understanding governing D-DEx/LInX allow for immediate use of some information under conditions of extreme danger, but follow up must be made with the originating agency as soon as possible.

3. Justification. All D-DEx users are required to provide a reason for the inquiry in the "justification" block of the search page. The purpose of the justification field is to remind the user why a query if question arise during an audit. To comply with Criminal Justice Information System (CJIS) requirements for the connection to N-DEx, LInX/D-DEx Version 5.2 now contains a requirement to use CJIS codes. Code "C" is used for normal criminal investigations, code "J" is used for criminal justice employment background checks, and code "A" is used for file administration such as compiling metrics on data from one's own agency.

a. Case control number (CCN). The CCN may be used in the justification block; however, a CCN is not always necessary. It is adequate to include sufficient information to remind users why they made the inquiry if questioned during an audit.

b. Reasons for investigation. Examples of proper justifications: "ID possible theft suspect," "locate witness," "get XYZ PD report number," "verify suspect's address," and "training." Entering "investigation" is not specific enough. "Testing" and "demonstration" are authorized for **HQ personnel only** if the query will include N-DEx. The reasons "Testing" and "demonstration" are allowed for all users if the selected neighborhoods **exclude** N-DEx agencies.

c. User cautions. Users are prohibited from running queries on themselves, acquaintances, or celebrities out of curiosity or for personal reasons. For training, users may run queries on convicted criminals or request sample queries from an RPM.

4. Background investigations. All D-DEx/LInX regional boards of governance prohibit the use of these systems for employment background investigations with the exception of background checks conducted on prospective employees or doing work for one's own law enforcement agency. Users should use the Code "J" for this purpose.

a. Category 2 investigations. Official D-DEx inquiries may be run during Category 2 investigations on NCIS employees or prospective employees. D-DEx may NOT be run for other purposes, such as general licensing, eligibility for federal or state benefits, or background investigations for other agencies or entities.

b. Background inquires in criminal investigations. The prohibited purposes listed in paragraph 4a of Appendix B do not apply to "background" inquiries of persons relevant to an investigation of criminal activities. If unique circumstances exist, contact a D-DEx Division representative for additional information.

5. Reporting results. When D-DEx/LInX/N-DEx information is summarized in an Investigative Action (IA) or otherwise documented by authorized inclusion, the user should indicate that the information was obtained from the contributing agency—not from D-DEx/LInX/N-DEx. Brief mentions in other reports are permitted:

a. General comment example. A user may put very general comments on D-DEx/LInX/N-DEx in NCIS reports to ensure thoroughness and to give context. For example, an NCIS ROI (OPEN) may contain this or similar language: "Reporting Agent queried the D-DEx/LInX/N-DEx systems, which showed that S/DOE was identified as being a victim of a burglary investigated by XYZ Police Department in 2006 under report # 123456. LInX records also indicated S/DOE was arrested for DUI by XYY PD in 2007 under citation number 34567 and FBI# XX34561. The official records of these incidents will be requested from XYZ and XYY Police Departments. No official action will be taken without the official documents or communications with the originating agency."

b. Permission to use queried information. The actual reports of the burglary and DUI should be sought from the police department, if relevant, and permission should be requested to include the actual report or a summary of it, per current NCIS report-writing policy.

6. Printing. Each regional Board of Governance, or N-DEx, determines its own printing rules.

a. Printing and retaining LInX copies. Local LInX governing bodies generally permit the temporary printing and retention of the copy for a period not to exceed 72 hours. These regional LInX rules are incorporated in the LInX operating system, which prevents printing or data inclusion if printing is not authorized from a particular region represented in the result set. Each printed document contains a caveat showing who printed the material and when it must be destroyed.

b. Printing and retaining D-DEx copies. Printing NCIS or DOD information from D-DEx is authorized for up to 72 hours.

c. Printed LInX/D-DEx results and case files. Printed D-DEx/LInX results are NOT to be filed in case files or attached to reports.

d. NCIS compliance monitoring. NCIS monitors compliance through the case review and audit processes.

7. Use of photographs. Most LInX regions and D-DEx permit printing photographs (mugshots) from the system. Photograph retention follows the same 72-hour restriction. If use of a photograph is needed for a longer period, the contributing agency should be contacted.

8. Audits. Each field office must audit D-DEx system use at least once a year. The assigned D-DEx RPM may conduct the audit and, with special agent in charge concurrence, enlist the assistance of field office personnel. The purpose of the audit is to maintain system integrity, not to discourage creative but appropriate use of the system. Audits will consist of a sampling of users. The system allows for precise auditing by username, date, and time. Questionable transactions will be researched and provided to the appropriate oversight entity. Misuse will be reported to the user's home agency and/or the applicable governance board, as necessary.

9. Sanctions. Unauthorized use, which includes requests, dissemination, sharing, copying, or receipt of D-DEx/LInX information, could result in civil proceedings against the offending

agency and/or criminal proceedings against any user or other person involved. Violations or misuse may also subject the user and the user's agency to administrative sanctions and possible disciplinary action by their agency. In addition to reporting through the chain of command, violations should be reported to the NCIS LInX/D-DEx Division.

NCIS-3 CHAPTER 47
REGIONAL ENFORCEMENT ACTION CAPABILITIES TEAM (REACT) PROGRAM
EFFECTIVE DATE: SEPTEMBER 2015

TABLE OF CONTENTS **PAGE**

References:

(a) NCIS-1, Chapter 34, Firearms, Intermediate Weapons, and Use of Force, January 2014
(b) NCIS-1, Chapter 13, Special Agent Career, March 2008
(c) NCIS-3, Chapter 39, Crisis Management and Hostage Negotiation, April 2008
(d) SECNAV Instruction 5430.107, Mission and Functions of the Naval Criminal Investigative Service, 28 December 2005

47-1. Purpose

a. This chapter addresses policy and procedures of the NCIS Regional Enforcement Action Capabilities Team (REACT) program and its personnel. Due to REACT personnel's training, tactics, procedures (TTPs), and the inherent nature of using and deploying tactical teams, this chapter may supersede existing restrictions and procedures contained in reference (a).

b. REACT's purpose is to support investigations and operations within the continental United States (CONUS) and to enhance the safety of the public, NCIS personnel, other law enforcement personnel, and subjects. The use of well-trained tactical teams to perform high-risk enforcement operations increases the probability of operational safety and success. The program's focus for NCIS offices outside the continental United States (OCONUS) is to support tactical training based on REACT TTPs.

47-2. Policy

a. Reference (a) discusses the primary DoD and Secretary of the Navy instructions outlining and assigning responsibilities affecting the NCIS agent corps and the REACT program. The REACT Program is responsible for training and certifying REACT personnel in advanced weaponry, to include less lethal platforms, chemical agent deployment, and unique munitions. Particular aspects of the program involving advanced weapons and use of force techniques postdates reference (a).

b. This chapter establishes policy, procedures, and guidelines regarding the use and management of the REACT program.

(b)(7)(E)

47-3. Cancellation. This chapter supersedes all local field office policies regarding the use and deployment of special response teams, special enforcement teams, and other tactical teams.

47-4. Chapter sponsor. NCIS Investigations and Operations, Code 23B.

47-5. Objectives

a. REACT program. The REACT program exists to preserve life, ensure public safety, enforce the laws within NCIS' jurisdiction, and assist with stabilizing the community affected by the operation or critical incident.

b. REACT team. The objectives of the REACT team are as follows:

(1) Conduct high-risk NCIS enforcement operations within the capabilities of the REACT Program as detailed in this policy.

(2) Support NCIS special agents during criminal investigations and operations to achieve NCIS objectives and missions.

(3) Provide tactical options to increase the likelihood of a safe and efficient resolution

of a situation, using maximum control while using the degree of force reasonably necessary to accomplish the law enforcement purpose in reacting to the subject(s)' actions.

(4) Implement procedures to use the specialization/expertise of needed NCIS resources, other law enforcement agencies, and outside experts (where appropriate) during crisis incidents (e.g., hostage situations, barricade incidents, etc.).

(5) Provide field offices (CONUS and OCONUS) and the NCIS Training Academy, Code 10B, with a pool of tactical instructors to increase NCIS' training and overall capabilities available to teach basic tactics during mandated monthly training for each CONUS field office, establish basic tactics to support the Special Agent Basic Training Program, and augment Code 10B with active-shooter response training through use of REACT active-shooter instructors.

47-6. Use/Functions

a. The REACT program is used in situations requiring specially equipped and trained personnel to effectively handle pre-planned high-risk enforcement operations or other identified missions where the tactical team concept provides an investigative and operational advantage.

b. REACT is a tactical team capable of performing a variety of operations, including:

(b)(7)(E)

47-7. Safety Priorities

a. These safety priorities are an important part of the decision-making process and must be considered when planning and executing REACT operations: hostages/victims, uninvolved members of the public, special agents/law enforcement officers, and subject(s).

b. Before a REACT operation, the special agent in charge (SAC), or their designee, will determine whether the action is reasonable and whether the operational need is warranted and in

accordance with established laws, NCIS policies, and procedures. This determination will be made using the NCIS operational threat matrix, a tool that will assist field office leadership quickly identify those operations that would benefit from the enhanced capabilities of a REACT team. The operational threat matrix is available on the REACT page on Lighthouse.

c. If REACT assistance is determined to be necessary, the SAC or designee will contact the REACT commander, or deputy commander if the commander is unavailable, for further discussion and evaluation. The DAD, Code 23B, maintains final approval authority for the use of REACT and the execution of a proposed operation.

47-8. General duties and responsibilities. Assignment to REACT is strictly voluntary and requires a positive attitude and tremendous commitment. This requires arduous physical training and the willingness to work and train for long hours. REACT is a collateral duty and does not take the place of current GS-1811 responsibilities and approved performance objectives. Responsibilities and requirements include the following:

a. Successful completion of the Basic REACT Operator's Course (BROC) and a probationary period. For more information on the selection process, see Appendix A.

b. Attendance and successful completion of all mandatory REACT quarterly training and certifications.

c. Successful completion of annual REACT physical fitness and quarterly firearms standards.

d. Individual performance appraisal (IPA) rating of "acceptable" or better.

e. Ability to participate in a coordinated tactical team response to any location in support of REACT operations/training.

f. Compliance with the NCIS policy on the use of force as described in reference (a) and REACT policies and procedures.

47-9. Composition. Each REACT team is organized, equipped, directed, and controlled by Code 23B, under the direction of the REACT commander. This ensures uniformity in administering and developing the REACT Program. Because of NCIS' changing needs and mobility, realignments of field offices, and geographical differences, the composition of each team may vary. The field office SAC may request changes in the total number of people assigned to a team through the Deputy Assistant Director (DAD), Code 23B. In general, each REACT team will be composed of one team leader (TL), one assistant team leader (ATL), and tactical operators.

47-10. Reviews

a. Each year, the REACT commander, deputy commander, and DAD, Code 23B, will conduct an administrative review of REACT management and recordkeeping procedures as well as review, in conjunction with each REACT TL, the tactical readiness of each team.

b. Each year, the REACT commander will conduct a review of the REACT program to validate proper standardized training goals, including the means to achieve those objectives.

c. At the conclusion of every REACT enforcement operation, the designated REACT TL will submit an after-action report (AAR) to the REACT commander and deputy commander. The report will be used to document compliance and measure program effectiveness.

Pages 1381 through 1404 redacted for the following reasons:
- -
(b)(7)(E)