



governmentattic.org

"Rummaging in the government's attic"

Description of document: Defense Criminal Investigative Service (DCIS) Special Agents Manual, 2016

Requested date: 31-December-2016

1st release: 22-March-2017
2nd release: 22-June-2017
3rd release: 25-July-2017
4th release: 21-September-2017

Posted date: 27-March-2017
Update posted: 24-September-2017

Note: Material released 22-June-2017 begins on PDF page 198
Material released 25-July-2017 begins on PDF page 465
Material released 21-Sep-2017 begins on PDF page 643

Source of document: FOIA Request
Department of Defense Office of Inspector General
DoD IG FOIA Requester Service Center
ATTN: FOIA/PA Chief, Suite 17F18
4800 Mark Center Drive
Alexandria, VA 22350-1500
Fax: (571) 372-7498
[FOIA Online](#)

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

March 22, 2017
Ref: DODOIG-2017-000193

SENT VIA EMAIL

This is an interim response to your Freedom of Information Act (FOIA) request for a copy of the Defense Criminal Investigative Service (DCIS) Special Agents Manual. We received your request on December 31, 2016, and assigned it case number DODIG-2017-000193.

The Defense Criminal Investigative Service conducted a search and found the enclosed documents, which consist of Chapters 1 through 15 of the Special Agents Manual, as responsive to your request. After carefully reviewing the records, I have determined that 155 pages of records are appropriate for release in full, copies of which are enclosed. Additionally, I have determined that 39 pages of records are appropriate for release in part, and that 441 pages of records are exempt from disclosure pursuant to: 5 U.S.C. § 552 (b)(6), which pertains to information, the release of which would constitute a clearly unwarranted invasion of personal privacy; 5 U.S.C. § 552 (b)(7)(C), which pertains to records or information compiled for law enforcement purposes, the release of which could reasonably be expected to constitute an unwarranted invasion of personal privacy; and 5 U.S.C. § 552 (b)(7)(E), which pertains to records or information compiled for law enforcement purposes, the release of which would disclose techniques and procedures for law enforcement investigations or prosecutions.

In view of the above interim response, you may consider this to be an adverse determination that may be appealed within 90 days of the date of this letter, however we recommend that you wait to submit any appeal until after a final response is sent to you. If you choose to appeal the interim release now, the appeal must be sent to the Department of Defense, Office of Inspector General, ATTN: FOIA Appellate Authority, Suite 10B24, 4800 Mark Center Drive, Alexandria, VA 22350-1500, postmarked within 90 days of this letter, and reference the file number above. I recommend that your appeal and its envelope both bear the notation "Freedom of Information Act Appeal."

March 22, 2017
Ref: DODOIG-2017-000193

Please be assured that you retain the right to appeal our final determination and, when we provide our final response, you will be afforded another 90 calendar days in which to appeal.

You may seek dispute resolution services and assistance with your request from the DoD OIG FOIA Public Liaison Officer at 703-604-9785, or the Office of Government Information Services (OGIS) at 877-684-6448, ogis@nara.gov, or <https://ogis.archives.gov/>. Please note that OGIS mediates disputes between FOIA requesters and Federal agencies as a non-exclusive alternative to litigation. However, OGIS does not have the authority to mediate requests made under the Privacy Act of 1974 (request to access one's own records.)

Please note that this office is continuing to process your FOIA request, and you will be provided responses on a rolling basis. If you have any questions regarding this matter, please contact Searle Slutzkin at 703-699-7520 or via email at foiarequests@dodig.mil.

Sincerely,

A handwritten signature in black ink, appearing to read "Mark Dorgan", with a long horizontal flourish extending to the right.

Mark Dorgan
Division Chief
FOIA, Privacy and Civil Liberties Office

Enclosure(s):
As stated

CHAPTER 1

ORGANIZATION, MISSION, JURISDICTION, AND AUTHORITIES

<u>Contents</u>	<u>Section</u>
General	1.1.
Organization	1.2.
Mission	1.3.
Exculpatory and impeachment information	1.4.
Jurisdiction	1.5.
Authorities	1.6.

1.1. General

1.1.a. This chapter introduces the Defense Criminal Investigative Service (DCIS), provides a historical overview, outlines the organizational structure and its relationship within the Department of Defense Inspector General (DoD IG), sets forth the jurisdiction, and defines the authorities of DCIS special agents. These policies and procedures are in accordance with the following references.

1.1.a.(1). Inspector General Act of 1978, as amended, (title 5 United States Code (U.S.C.), Appendix 3).

1.1.a.(2). Department of Defense (DoD) Directive 5106.01, “Inspector General of the Department of Defense,” April 20, 2012.

1.1.a.(3). Title 10 U.S.C. section 1585a, “Special agents of the Defense Criminal Investigative Service: authority to execute warrants and make arrests.”

1.1.a.(4). Manual for Courts-Martial (2012 Edition), United States, Chapter III, Rule 302, Apprehension.

1.1.a.(5). DoD Instruction 5505.02, “Criminal Investigations of Fraud Offenses,” August 29, 2013.

1.1.a.(6). DoD Instruction 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,” June 18, 2007.

1.1.a.(7). DoD Instruction 5525.12, “Implementation of the Amended Law Enforcement Officers Safety Act of 2004 (LEOSA),” February 13, 2014.

1.1.a.(8). DoD Inspector General Memorandum, “Delegation of Authority to Establish Defense Criminal Investigative Service Policy,” March 14, 2011. See <https://intra.dodig.mil/inv/sam/Delegation%20of%20Authority.pdf> on the DoD IG Intranet.

1.1.a.(9). DoD Instruction 7050.03, “Office of the Inspector General of the Department of Defense Access to Records and Information,” March 22, 2013.

1.1.b. The Secretary of Defense established DCIS on April 20, 1981. The criminal investigative functions assigned to the Defense Investigative Service, now known as the Defense Security Service, were transferred, along with 100 personnel billets, to the Office of the Assistant to the Secretary of Defense (Review and Oversight). In October 1981, an initial cadre of 12 individuals of the DIS Special Investigations Unit began operations under the direction, authority, and control of the Assistant to the Secretary of Defense (Review and Oversight). DCIS was established as a worldwide civilian Federal law enforcement agency to investigate suspected criminal activities involving DoD Components and DoD contractors.

1.1.c. When the Inspector General Act of 1978 was amended to include DoD, the position of Assistant Inspector General for Investigations (AIGI) was established. Before 2002, the AIGI also served as the Director, DCIS. In 2002, separate positions were established for the AIGI and Director, DCIS. Later, the title of the AIGI was changed to Deputy Inspector General for Investigations (DIG-INV). When DCIS was reorganized in 2010, the Director position was eliminated and replaced with a three-person AIGI structure. In 2013, a policy was established for the following positions to use dual titles (Attachment A):

1.1.c.(1). The DIG-INV was cross-designated as Director, DCIS.

1.1.c.(2). The AIGIs were cross-designated as Deputy Directors of DCIS.

1.1.c.(3). Special Agents in Charge (SACs) assigned to DCIS Headquarters were referred to as Deputy Assistant Inspectors General for Investigation (DAIGIs) and cross-designated as Assistant Directors of DCIS.

1.1.d. The Inspector General of the Department of Defense (Inspector General, DoD) serves as the principal advisor to the Secretary of Defense on investigative matters covered by the Inspector General Act of 1978, as amended, and for matters relating to the prevention and detection of fraud, waste, and abuse in DoD programs and operations.

1.2. Organization

1.2.a. The DoD IG is composed of the IG, a Principal Deputy IG (PDIG), and seven Deputy Inspectors General (DIGs), as depicted on the DoD IG website.

1.2.b. DCIS consists of a Headquarters and subordinate field offices (FOs) throughout the United States. The FOs, subordinate resident agencies (RAs), and posts of duty (PODs) are in locations where Defense Agencies have primary field-level elements and/or where a DCIS

presence is required to support national defense priorities. A listing of DCIS field components is on the DoD IG Intranet at <http://www.dodig.mil/Map/DCIO/dcismap.html>.

1.2.c. The DIG-INV is responsible for overall control and direction of the organization. Under the direction of the DIG-INV, the DCIS Headquarters staff provides oversight and support to all DCIS investigative elements in three functional areas headed by AIGIs, as follows:

- AIGI, Investigative Operations Directorate
 - DAIGI, Investigative Operations
 - Regional FO SACs (x6)
- AIGI, International Operations Directorate
 - DAIGI, International Operations
 - SAC, Cyber FO
- AIGI, Internal Operations Directorate
 - DAIGI, Internal Operations

1.2.c.(1). The AIGIs provide direction to individual directorates and serve as the first-line supervisors of DAIGIs. The AIGI for Investigative Operations serves as the first-line supervisor to regional FO SACs. The DCIS Headquarters directorates provide operational guidance, program-specific oversight, and coordination; review operations and investigations; and ensure proper information flow, essential to the successful execution of the DCIS mission, through significant liaison efforts.

1.2.c.(1).(a). The Investigative Operations Directorate provides oversight, coordination, and support to all DCIS investigative elements in the functional program areas of regional operations, special operations, and asset forfeiture. This directorate provides guidance to the field on all investigative issues, coordinates policy in the functional areas, and develops conference and training opportunities for the field. Additionally, the AIGI for Investigative Operations serves as the first-line supervisor of the DAIGI, Investigative Operations, and all regional FO SACs.

1.2.c.(1).(b). The International Operations Directorate provides oversight, coordination, and support to DCIS investigative elements in the functional program areas of international affairs, national security, and cyber crimes. This directorate also provides guidance to the field on investigative issues, coordinates policy in these functional areas, manages the deployment process, and develops conference and training opportunities for the field. Additionally, the AIGI for International Operations serves as the first-line supervisor of the DAIGI, International Operations, and SAC, Cyber Crimes FO.

1.2.c.(1).(c). The Internal Operations Directorate maintains computerized management information systems, provides studies of trends developed from criminal investigations, and conducts management inquiries concerning complaints against DCIS personnel on matters not pursued by the Office of Quality Assurance and Standards. (See IG Instruction 1400.4, “Adverse Actions,” March 5, 2014, for further guidance regarding disciplinary and adverse actions policies.) The Internal Operations Directorate is responsible for

all training, including use of force and defensive tactics, through the Training Division at the Federal Law Enforcement Training Center, Glynco, Georgia. It is also responsible for policy, space management for DCIS offices, and all logistics related to agent safety, defensive tactics, and use of force equipment. The Internal Operations Directorate provides logistical and administrative support to Headquarters DCIS and all field elements and conducts liaison and marketing to enhance the public's knowledge of DCIS and to recruit quality DCIS personnel. Additionally, the AIGI for Internal Operations serves as the first-line supervisor of the DAIGI, Internal Operations.

1.3. Mission

1.3.a. The DCIS mission is to conduct highly relevant, objective, professional investigations of matters critical to DoD property, programs, and operations that provide for our national security with emphasis on life, safety, and readiness.

1.3.b. As the criminal investigative arm of the DoD IG, DCIS accomplishes its mission by investigating suspected criminal violations in the priority areas as determined annually by the DIG-INV, in conjunction with the priorities set by the Inspector General, DoD and the Secretary of Defense, and by conducting DCIS mission briefings in all elements of DoD.

1.3.c. DCIS activities are also governed by the U.S. Constitution, case law, and statutes related to criminal investigations. Special agents must consistently ensure they respect and protect individuals' constitutional rights, including the right to due process.

1.4. Disclosure of Exculpatory and Impeachment Information.

1.4.a. **Exculpatory Information.** Government disclosure of material exculpatory and impeachment evidence is part of the constitutional guarantee to a fair trial. (See *Brady v. Maryland*, 373 U.S. 83, 87 (1963); *Giglio v. United States*, 405 U.S. at 150, 154 (1972)). The law requires the disclosure of exculpatory and impeachment evidence when such evidence is material to guilt or punishment, as found in *Brady v. Maryland*, 373 U.S. at 87, and *Giglio v. United States*, 405 U.S. at 154. Because they are Constitutional obligations, *Brady* and *Giglio* evidence must be disclosed regardless of whether the defendant makes a request for exculpatory or impeachment evidence. (See *Kyles v. Whitley*, 514 U.S. 419, 432-33 (1995)). Special agents must disclose to the assigned prosecutors and/or appropriate legal authorities exculpatory information reasonably promptly after it is discovered in their investigations. This information will be documented and maintained in the official case file when applicable. (See Special Agents Manual (SAM) Chapter 28, "Investigative Reports," for guidance on report writing.)

1.4.b. **Giglio/Henthorn.** The Government has an obligation to disclose favorable material evidence. The failure to disclose such evidence may violate due process. The Supreme Court ruled in *Giglio v. United States*, 405 U.S. 150 (1972), that the "reliability of a given witness may well be determinative of guilt or innocence..." Later, in *United States v. Henthorn*, 931 F.2d 29 (9th Cir. 1991), the Court held that the Government is required to review the personnel files of law enforcement officials whom the Government intends to call as witnesses to

uncover any potential impeachment material. Thus, it is DCIS's policy that every DCIS special agent is obligated to inform criminal DOJ trial attorneys/Assistant United States Attorneys (AUSA) with whom the agent works and their DCIS supervisory chain of command of "potential impeachment information" as soon as it is known to the DCIS special agent, but under no circumstances later than immediately before providing a sworn statement or testimony in any criminal investigation or case. The United States Attorney's Manual (USAM), Section 9-5.100, (the "Giglio Policy"), updated July 2014, states:

The exact parameters of potential impeachment information are not easily determined. Potential impeachment information, however, has been generally defined as impeaching information which is material to the defense. *It also includes information that either casts a substantial doubt upon the accuracy of any evidence—including witness testimony—the prosecutor intends to rely on to prove an element of any crime charged, or might have a significant bearing on the admissibility of prosecution evidence.* This information may include but is not strictly limited to: (a) specific instances of conduct of a witness for the purpose of attacking the witness' credibility or character for truthfulness; (b) evidence in the form of opinion or reputation as to a witness' character for truthfulness; (c) prior inconsistent statements; and (d) information that may be used to suggest that a witness is biased.

If a DCIS special agent has any question whether potential impeachment information qualifies for disclosure, the information should be disclosed. DCIS special agents should refer to the USAM's Giglio Policy for the most up to date categories of potential impeachable information.

1.4.c. If a supervisor has knowledge of any potential impeachment information related to any special agent under his/her supervision, the supervisor will remind the special agent of the requirements to notify the appropriate prosecutors as early as possible prior to serving as an affiant or witness in any case or matter.

1.5. Jurisdiction

1.5.a. Pursuant to the Inspector General Act of 1978, as amended, DCIS has broad criminal investigative jurisdiction for DoD programs and operations. DCIS jurisdiction includes any investigation that ensures the integrity of the procurement system from fraud and other criminal violations, such as public corruption; financial crimes; product substitution; health care fraud; computer crimes; and the illegal theft, export, diversion, transfer, or proliferation of DoD technology. This involves the entire procurement process, from initial research and development to the disposal of products no longer needed by DoD units and operations.

1.5.b. DoD Instruction 5525.07 implements a 1984 MOU between DoD and DOJ. The MOU sets forth responsibilities in particular types of cases. Provisions of special note are as follows.

1.5.b.(1). Allegations of "bribery and conflict of interest...[involving] present, retired, or former General or Flag Officers and civilians in positions above the GS-15 and

equivalent levels, the Senior Executive Service, and the Executive Level” should be referred to the Federal Bureau of Investigation (FBI) on receipt. Consideration for referral of other “significant” corruption allegations shall be based on the gravity of the circumstances—e.g., “sensitivity of the DoD program involved, amount of money in the alleged bribe, number of DoD personnel implicated, [and] impact on the affected DoD program.” Consideration should also be given to working jointly with the FBI in these investigations. DCIS will handle all other bribery allegations in accordance with standard operating procedures.

1.5.b.(2). When DCIS investigations uncover evidence of fraud against DoD and/or theft and embezzlement of Government property, DCIS special agents should confer with the DOJ prosecutor (usually an AUSA) and notify the FBI of the meeting. In consultation with DoD, the DOJ prosecutor will determine criminal investigative responsibility. A DCIS investigation brought to the attention of the DOJ Federal Procurement Fraud Unit will satisfy the “conference” requirements as to both the prosecutor and the FBI.

1.5.b.(3). For crimes committed on military installations in the United States, the concerned DoD criminal investigative organization will investigate all crimes (other than certain bribery and conflict of interest allegations described in paragraph 1.5.b.(1).) in which the subject(s) can be tried by court-martial or are unknown. However, DoD investigative organizations shall immediately notify DOJ of cases falling within the prosecutorial guidelines of the local United States Attorney in which an individual subject/victim is not a military member or dependent. In any criminal case, if one or more subjects cannot be tried by court-martial, immediately notify the FBI.

1.5.c. Within DoD, the criminal investigative jurisdiction of DCIS for fraud offenses is set forth in DoD Instruction 5505.02, as follows:

1.5.c.(1). The Office of the Secretary of Defense (OSD), Defense Agencies, and DoD Field Activities.

1.5.c.(2). The Chairman of the Joint Chiefs of Staff (CJCS) and Vice CJCS.

1.5.c.(3). All contract and procurement actions awarded by DoD Components and Field Activities, with the exception of those for which Military Criminal Investigative Organizations (MCIOs) have responsibility.

1.5.c.(4). All Defense Logistics Agency (DLA) disposition services and DLA distribution activities, with the exception of those specified in paragraph 2d of this enclosure. DCIS must, except under urgent circumstances, notify, within 72 hours, the cognizant MCIO office that an investigation has begun under this provision regarding a DLA disposition service or DLA distribution activity on any installation covered in paragraph 2d of this enclosure. DCIS must accomplish any notice to, or briefing of, the installation commander with the participation of the cognizant MCIO.

1.5.c.(5). All allegations of fraud committed by health care providers, including “partnership agreement” situations under the Defense Health Agency (formerly TRICARE Management Activity) and fiscal intermediaries. If the allegations concern a provider on a specific military installation or activity, notify the appropriate MCIO.

1.5.c.(6). Allegations of suspected violations of the Anti-Kickback Act (41 U.S.C. §§ 8701 through 8707) that contractors are required to report under that statute, whether or not they do so. If allegations concern a specific Military Department, DCIS will promptly notify the concerned Department, through the appropriate MCIO, when it initiates an investigation affecting that Department’s personnel, activities, or contracts, or when it discovers any suspected Uniform Code of Military Justice (UCMJ) violations. The exception to this notification requirement is when the Inspector General, DoD, or his or her designee, determines such notification is not appropriate. Likewise, an MCIO will promptly notify the DCIS when it initiates an investigation affecting the personnel, activities, or contracts of the OSD, Office of the CJCS, or other matters under DCIS’s primary jurisdiction as outlined in this instruction. This notification requirement should not limit the DoD IG statutory authority to conduct investigations in a manner deemed appropriate by the Inspector General, DoD.

1.5.c.(7). All kickbacks (41 U.S.C. §§ 8701 through 8707) or bribery (18 U.S.C. § 201) involving civilian employees of OSD, the Joint Staff, Defense Agencies, and DoD Field Activities.

1.5.c.(8). Any allegations that the Inspector General, DoD considers appropriate for investigation by DCIS.

1.5.d. DoD Instruction 5505.02, Enclosure 3, paragraph 8, states that DCIS may share fraud investigative jurisdiction with the MCIOs under the following circumstances.

1.5.d.(1). The alleged fraud substantially involves and impacts the funding, programs, property, or personnel (as subjects) of more than one DoD Component.

1.5.d.(2). The nature of the investigation requires the commitment of more resources than a single Defense Criminal Investigative Organization (DCIO) can reasonably provide to the investigation.

1.5.d.(3). The DCIO that wants to join the investigation has and will provide sufficient resources to actively contribute to the investigative team.

1.5.d.(4). DoD-level policy or a memorandum of understanding applicable to the case requires more than one DCIO to participate in the investigation.

1.5.d.(5). The investigation involves a TRICARE provider on a military installation.

1.5.d.(6). The matter being investigated is considered to be of such importance to a Military Department that participation by more than one DCIO may avoid any appearance of conflict of interest, lack of independence, or possible command influence.

1.5.d.(7). The DoD IG determines that an investigation will be conducted jointly or that DCIS must be a joint participant in an investigation with another DCIO.

1.6. Authorities. DCIS responsibilities as an organization are set forth in the Inspector General Act of 1978, as amended, and DoD Directive 5106.01. The responsibilities of each field component are predominantly assigned on a geographical basis and at Headquarters on a program basis. This section highlights certain authorities of each DCIS special agent that are not contained elsewhere in the SAM.

1.6.a. Administration of Oaths. The authority for DCIS personnel to administer oaths is in 5 U.S.C. § 303.

1.6.b. IG Subpoenas and Other Access to Information. The authority of the DoD IG to obtain records, documents, and the attendance and testimony of witnesses by subpoena is found in the Inspector General Act of 1978, as amended, and is described in detail in SAM Chapter 13, “Inspector General Subpoena Guidelines.” Sometimes, however, records and documents from other Federal agencies are required. The Inspector General Act of 1978, as amended, provides “[t]hat procedures other than subpoenas shall be used by the Inspector General to obtain documents and information from Federal agencies.” DoD Directive 5106.01 states that within DoD, the DoD IG shall “[a]ccess all records (electronic or otherwise), reports, investigations, audits, reviews, documents, papers, recommendations, or other information or material available to any DoD Component.” Furthermore, “Except as specifically denied in writing by the Secretary of Defense...no officer, employee, or Service member of any DoD Component may deny the IG DoD [sic], or officials assigned by the IG DoD [sic], access to information, or prevent them from conducting an audit, evaluation, inspection, or investigation.” The IG Act of 1978, as amended, states that the DoD IG shall have expeditious and unrestricted access to all records, reports, and so forth with the exception of:

1.6.b.(1). sensitive operational plans,

1.6.b.(2). intelligence matters,

1.6.b.(3). counterintelligence matters, and

1.6.b.(4). ongoing criminal investigations by other DoD administrative units related to national security.

In regard to records of Federal agencies other than DoD, the Inspector General Act of 1978, as amended, states that “[u]pon request of an Inspector General for information or assistance . . . the head of any Federal agency involved shall, insofar as is practicable and not in contravention of any existing statutory restriction or regulation of the Federal agency from which the information

is requested, furnished to such Inspector General, or to an authorized designee, such information or assistance.”

1.6.c. Firearms. Authority for DCIS special agents to carry firearms is based on 10 U.S.C. § 1585 and is fully addressed in SAM Chapter 38, “Use of Force.” DCIS special agents are also covered by the provisions of LEOSA, as stated in DoD Instruction 5525.12.

1.6.d. Arrest Authority. Authority for DCIS special agents to make arrests is based on 10 U.S.C. § 1585a. This authority and related procedures are fully described in SAM Chapter 20, “Arrests.” Authority for DCIS special agents to apprehend military personnel is in Chapter III, Rule 302 of the Manual for Courts-Martial, United States (Revised edition 2012). In general, any DCIS special agent conducting an investigation under DCIS jurisdiction may apprehend persons subject to the UCMJ on reasonable belief an offense has been committed and that the person to be apprehended has committed it. A person so apprehended should be delivered promptly to his/her commanding officer or other appropriate military authority.

1.6.e. Search Warrants. Authority for DCIS special agents to execute search warrants is also based on 10 U.S.C. § 1585a. This authority and related procedures are fully described in SAM Chapter 19, “Searches.” The authority of DCIS special agents to request issuance of a Federal search warrant is found in title 28, Code of Federal Regulations (CFR), Chapter 1, Section 60.3(a)(2). This section, under the general heading “Department of Defense,” identifies the Office of Assistant Inspector General for Investigations of the Office of Defense Inspector General as an agency with law enforcement officers authorized to request the issuance of search warrants. Rule 41 of the Federal Rules of Criminal Procedure relates to Searches and Seizures.

1.6.f. Coverage Designation for Federal Officers. Title 28, CFR, Chapter 1, Section 64.2(h) designates DCIS special agents for coverage under 18 U.S.C. § 1114, which states, “[w]hoever kills or attempts to kill any officer or employee of the United States or of any agency in any branch of the United States Government (including any member of the uniformed services) while such officer or employee is engaged in or on account of the performance of official duties, or any person assisting such an officer or employee in the performance of such duties or on account of that assistance, shall be punished (1) in the case of murder, as provided under section 1111; (2) in the case of manslaughter, as provided under section 1112; or (3) in the case of attempted murder or manslaughter, as provided in section 1113.”

ATTACHMENTS

- A Dual Designations – DCIS Leader Positions, May 3, 2013.

ATTACHMENT A



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

ACTION MEMO

May 3, 2013

FOR PRINCIPAL DEPUTY INSPECTOR GENERAL

FROM: James Burch, Deputy Inspector General for Investigations

SUBJECT: Dual Designations – DCIS Leader Positions

- In the past, the Deputy Inspector General for Investigations also held the title of DCIS Director. This “dual-designation” policy enhanced the DIGI’s ability to effectively interact with counterparts throughout the traditional law enforcement community, as well as the Inspector General community. This action memo requests your approval to reinstitute this policy.
- Upon receiving your approval, the following individuals will utilize dual titles:
 - The Deputy Inspector General for Investigations will be cross-designated as Director, DCIS.
 - Assistant Inspectors General for Investigations will be cross-designated as Deputy Directors of DCIS.
 - Special Agents in Charge assigned to DCIS Headquarters will be referred to as Deputy Assistant Inspector Generals for Investigation and cross-designated as Assistant Directors of DCIS.
- Implementing this proposal will *not* require position description adjustments and/or performance plan modifications. The proposed changes are strictly cosmetic; however, I believe they will enhance DCIS leaders’ ability to effectively interact with counterparts.
- RECOMMENDATION: PDIG approve this proposal by initialing and dating the ACTION below.

Approve (b)(6), (b)(7)(C) 5/23/13 Disapprove _____ Other _____
Initial Date Initial Date Initial Date

COORDINATION: _____ Initial Date

DoD IG General Counsel (b)(6), (b)(7)(C)
Office of Executive and Leader Talent Management (b)(6), (b)(7)(C)

Prepared By: (b)(6), (b)(7)(C) Assistant Inspector General for Investigative Operations, 604-6, (b)(7)

~~FOR OFFICIAL USE ONLY~~

#OIM 013832-13

CHAPTER 2

SENSITIVE INVESTIGATIONS PROGRAM

<u>Contents</u>	<u>Section</u>
General	2.1.
Definitions	2.2.
Program Objectives	2.3.
Sensitive Investigations	2.4.
Y0 (Security Violations) Investigations Restrictions	2.5.
Classified Report Preparation	2.6.
Training Requirements	2.7.
System of Records	2.8.
Classified Evidence	2.9.
SAP Cadre	2.10.
SCI Eligibility and Access	2.11.
Passing Security Clearances	2.12.
Access to SAPs	2.13.
Courier Cards	2.14.

2.1. General

2.1.a. **Purpose.** This chapter outlines policies and procedures governing the Defense Criminal Investigative Service (DCIS) Sensitive Investigations Program. The Program is designed to provide guidance, support, and oversight to DCIS agents conducting Sensitive Investigations as defined in 2.4. The Program will also manage the DCIS Special Access Program (SAP) cadre, a small group of seasoned agents with special training allowing them to respond to referrals involving fraud, waste, and abuse within a DoD SAP.

2.1.b **Classified Information.** Executive Order 13526, “Classified National Security Information,” identifies three types of classified information:

2.1.b.(1). **Confidential.** Confidential information is information, the unauthorized disclosure of which could reasonably be expected to cause damage to national security.

2.1.b.(2). **Secret.** Secret information is information, the unauthorized disclosure of which could reasonably be expected to cause *serious* damage to national security.

2.1.b.(3). **Top Secret.** Top Secret information is information, the unauthorized disclosure of which could reasonably be expected to cause *exceptionally grave* damage to national security.

2.2. Definitions

2.2.a. **Intelligence Community (IC).** The U.S. IC is a coalition of 17 agencies and organizations within the Executive Branch that work both independently and collaboratively to gather and analyze the intelligence necessary to conduct foreign relations and national security activities. The 17 members of the IC are the Office of the Director of National Intelligence (ODNI), Air Force Intelligence, Army Intelligence, Central Intelligence Agency (CIA), Coast Guard Intelligence, Defense Intelligence Agency (DIA), Department of Energy, Department of Homeland Security, Department of State, Department of Treasury, Drug Enforcement Administration, Federal Bureau of Investigation, Marine Corps Intelligence, National Geospatial Intelligence Agency (NGA), National Reconnaissance Office (NRO), National Security Agency (NSA), and Navy Intelligence.

2.2.b. **DoD Intelligence Community.** The subset of eight IC members that fall under the DoD: Air Force Intelligence, Army Intelligence, DIA, Marine Corps Intelligence, NGA, NRO, NSA, and Navy Intelligence.

2.2.c. **Special Access Program (SAP).** DoD Directive 5205.07, “Special Access Program (SAP) Policy,” July 1, 2010, and DoD Instruction 5205.11, “Management, Administration, and Oversight of DoD Special Access Programs (SAPs),” February 6, 2013, provide overarching guidance for DoD SAPs. SAPs are security protocols that provide highly classified information, capabilities, technologies, and operations with safeguards and access restrictions exceeding those for regular (collateral) classified information. All DoD SAPs are approved by the Secretary of Defense (SECDEF) or Deputy Secretary of Defense (DEPSECDEF). The DoD Special Access Program Central Office (SAPCO) administers SAPs for the DoD. SAP material may only be viewed by individuals who have been specifically adjudicated and accessed to the material in the SAP and may only view the material in a space specifically designated by SAPCO as a SAP Facility (SAP-F). DCIS Field Offices are not accredited to store or review any SAP material.

There are three types of SAPs defined in DoD Directive 5205.07:

2.2.c.(1). **Acknowledged SAP.** A SAP whose existence is acknowledged, affirmed or made known to others, but its specific details (technologies, materials, techniques, etc.) are classified as specified in the applicable security classification guide.

2.2.c.(2). **Unacknowledged SAP.** A SAP having enhanced security measures ensuring the existence of the program is not acknowledged, affirmed, or made known to any persons not authorized for such information.

2.2.c.(3). **Waived SAP.** A SAP for which the Secretary of Defense has waived the applicable reporting requirements in accordance with DoD Manual 5200.01, “DoD Information Security Program,” February 24, 2012, as amended, following a determination of adverse effect to national security. An unacknowledged/waived SAP that has more restrictive reporting and access controls than other unacknowledged SAPs.

2.2.d. Sensitive Compartmented Information (SCI). SCI is a type of Top Secret classified information concerning or derived from sensitive intelligence sources, methods or analytical processes. It is not a classification in and of itself, but rather is a system of enhanced access controls. Eligibility for access to SCI requires review and adjudication beyond that required for a Top Secret security clearance. SCI material may only be viewed in a space designated as a Sensitive Compartmented Information Facility (SCIF). DCIS Field Offices are not approved to store or review Top Secret or Top Secret SCI material. However, given the oversight responsibilities inherent in the Resident Agent in Charge (RAC), all RACs who supervise agents with access to TS/SCI shall also have a TS clearance with access to SCI.

2.2.e. Secret Internet Protocol Router Network (SIPRnet). SIPRnet is the DoD computer network for the exchange of classified material up to the SECRET level.

2.2.f. Joint Worldwide Intelligence Communications System (JWICS). JWICS is the DoD computer network for the exchange of classified material up to the Top Secret/SCI level.

2.2.g. Counterintelligence (CI). Presidential Executive Order 12333 defines counterintelligence as “information gathered and activities conducted to identify, deceive, exploit, disrupt or protect against espionage, other intelligence activities, sabotage or assassinations conducted for or on behalf of foreign powers, organizations or persons, or their agents or other international terrorist organizations or activities.” DCIS does not have a CI mission/chapter, thus DCIS does not engage in CI investigations. However, there will be occasions in which a criminal investigation parallels a CI investigation. It is imperative that DCIS agents coordinate and deconflict such cases with the cognizant CI investigative authority.

2.2.h. Alternative Compensatory Control Measures (ACCM). ACCMs provide additional access control measures to classified information when standard classification is insufficient to enforce need to know and SCI or SAP protections are not warranted. The use of an unclassified nickname, together with a list of persons authorized access, and a specific description of information subject to the enhanced ACCM controls, are the three requisite elements of an ACCM.

2.3. Program Objectives

2.3.a. Perform oversight on a body of investigations that, by virtue of classified elements and information, have unique reporting, training, handling, and storage requirements.

2.3.b. Ensure that cases opened within this body of investigations adhere to DCIS investigative priorities and strictly adhere to DoD policies and procedures regarding classified information.

2.3.c. Ensure agents working these investigations are properly trained and have proper infrastructure to perform their jobs in accordance with current DoD policy.

2.3.d. Maintain headquarters level liaison with Inspectors General and other investigative bodies within the DoD Intelligence Community.

2.3.e. Maintain headquarters level liaison with DoD Counterintelligence entities for deconfliction and to identify opportunities for parallel investigations.

2.4. Sensitive Investigations

2.4.a. **Definition.** The term “Sensitive Investigations” means any case identified below, regardless of which specific DCIS case category the investigation falls within:

2.4.a.(1). All DCIS investigations involving a SAP or SAPs;

2.4.a.(2). All DCIS investigations requiring agents to review, analyze, process, store, or create classified information;

2.4.a.(3). All DCIS investigations involving personnel and programs administered by agencies of the Intelligence Community regardless of the actual classification level of the material involved; and

2.4.a.(4). All DCIS investigations that “parallel” an ongoing Counterintelligence investigation by another agency. “Parallel” means that DCIS and another agency are actively coordinating and deconflicting the criminal investigation with the counterintelligence operation. The mere existence of a relevant counterintelligence operation, absent any active coordination or deconfliction by DCIS, does not constitute a parallel investigation.

2.5. Y0 (Security Violations) Investigations Restrictions

2.5.a. The following types of classified/sensitive issues do not typically fall under the purview of the Y0 case category (Security Violations) and should be opened by DCIS on a very limited basis and only with DCIS Headquarters approval:

2.5.a.(1). Counterintelligence matters;

2.5.a.(2). Espionage matters;

2.5.a.(3). Individual loss/mishandling/spillage of classified information regardless of the actual classification level of the information involved;

2.5.a.(4). Issues involving individual suitability for access to classified information; and

2.5.a.(5). Issues involving individual security violations.

2.6. Classified Report Preparation

2.6.a. Any DCIS report containing classified material will be properly marked in accordance with DoD Manual 5200.01, “DoD Information Security Program: Overview, Classification, and Declassification,” February 24, 2012; DoD 5200.1-PH, “DoD Guide to Marking Classified Documents,” April 1, 1997; DoD 5205.07 v4, “Special Access Program (SAP) Security Manual,” October 10, 2013; and IGDINST 5200.1, “Information Security Program,” August 31, 2007. Under no circumstances will the official unclassified case file contain classified information, and under no circumstances will classified documents be

uploaded to CRIMS. Contact the Program Manager, Sensitive Investigations, for further guidance regarding the preparation, marking, storage, accountability, reproduction, transmission, transportation, or disposal of any classified case documents.

2.7. Training Requirements

2.7.a. Derivative Classification Training. In accordance with DoDM 5200.01, Volume 3, Enclosure 5, paragraph c, “Derivative classifiers (i.e., those who create new documents, including e-mails, based on existing classification guidance) shall receive training in derivative classification, with an emphasis on avoiding over-classification, at least once every 2 years.” Given that all special agents possess Top Secret security clearances, this training requirement shall apply to all DCIS Special Agents. The two hour web-based training course is available through the DoD IG Office of Security (OSEC). Training completion and dates will be tracked by the OSEC Information Security Manager.

2.8. System of Records

2.8.a. General. It is the responsibility of every DCIS special agent working with classified information to know and follow the applicable directives and guidance. Volume 1 of DoD Manual 5200.01 states, “All personnel of the Department of Defense are personally and individually responsible for properly protecting classified information... All officials within the Department of Defense who hold command, management, or supervisory positions have specific, non-delegable responsibility for the quality and effectiveness of implementation and management of the information security program within their areas of responsibility.” Any questions concerning the handling, processing, transmission, or storage of classified material involved in DCIS Classified Investigations should be referred to the Program Manager, Classified Investigations.

2.8.b. CRIMS Entries. Special Agents Manual (SAM) Chapter 50, “Case Reporting and Information Management System,” states “CRIMS is an unclassified system and, therefore, **only unclassified information can be collected in CRIMS.**” When DCIS personnel are working a classified investigation, only unclassified information will be reported in CRIMS. See SAM Chapter 50 for guidance on creating a shell case record, including the minimum requirements, and for guidance on titling unclassified subjects.

2.8.c. Sensitive Investigations Special Interest Code (SIC). All DCIS investigations meeting the definition of a Sensitive Investigation will incorporate the “Sensitive Investigation” Special Interest Code in CRIMS.

2.8.d. Unclassified Placeholders in CRIMS. When a Case Initiation Report (CIR) itself is classified, it will **not** be uploaded to CRIMS. Instead, an unclassified “place holder” will be uploaded to CRIMS. The unclassified “place holder” will contain the standard Form 1 header (Full case number, date and subject). The body of the report will state, “This is a classified investigation. For access to this investigation, please contact the DCIS Program Manager for Classified Investigations.”

2.8.e. Creation of Classified Reports. Classified information cannot be processed on unclassified information technology (IT) systems. The following are authorized systems for processing classified information to include DCIS investigative reports:

2.8.e.(1). *Confidential or Secret*: SIPRNET, or an authorized/approved standalone computer at the Secret level.

2.8.e.(2). *Top Secret or TS/SCI*: JWICS, or an authorized/approved standalone computer at the TS or TS/SCI level.

2.8.e.(3). *SAP Material*: An IT system or standalone computer specifically authorized by SAPCO for processing SAP material.

2.8.f. Storage of Classified Reports. Classified investigative case files should be maintained in accordance with Chapter 42 of the Special Agents Manual, however, classified case files must be stored in accordance with DoD Manual 5200.01, Volume 3 and IGDINST 5205.7. Unclassified reports may be entered into a classified case file, but the case file itself must be handled and stored at the highest level of classification contained within the file.

2.9. Classified Evidence

2.9.a. Evidence Custody System (ECS). SAM Chapter 18 addresses classified evidence issues, stating in part “Classified documents may be maintained in the ECS, if necessary, as long as all appropriate information security regulations are followed. However, the procedures of this chapter do not apply to Special Access Program documents, TS documents, or TS/SCI documents that are acquired as evidence. In such cases, the special agent should work with the Program Director, National Security and the appropriate program security office to develop procedures that will adequately address the chain of custody issues for the documents.”

2.10. SAP Cadre

2.10.a. DoD Directive 5205.07, SAP Policy. DoD Directive 5205.07, states in part “The IG DoD shall maintain a sufficient dedicated cadre of SAP-trained personnel to perform inspection, investigation, evaluation, and audit functions for DoD SAPs and SAP-related activities.”

2.10.b. Centralized SAP Cadre. The DCIS SAP Cadre will consist of specially designated and trained special agents. The SAP Cadre will be responsible for all DCIS investigations involving SAPs and all DCIS investigations requiring agents to review, analyze, process, store, or create classified information at the level of Top Secret and Top Secret/SCI. On a case by case basis, the Program Director, National Security may direct the SAP Cadre to work other Classified Investigations upon request of supervisors in the field or other DoD IG entities.

2.10.c. Selection of SAP Cadre. Is being developed and will initially be published as an Interim Policy until incorporated into the next revision of this Chapter.

2.10.d. SAP Cadre Training. DCIS has identified the Defense Security Service Phase I “Introduction to Special Access Programs,” curriculum as the required base level training for

special agents before conducting any investigation involving a SAP. Phase 1 is a series of online courses including: Introduction to Information Security, Introduction to Personnel Security, Marking Classified Information, Special Access Program Overview, Defining OPSEC in SAPs, Security Compliance Inspection Process, Special Access Program Security Incidents, Packaging Classified Documents, Developing a Security Education and Training Program, Transmission and Transportation for DoD, and Introduction to Physical Security. Most of these courses require a passing score on an exam. The Program Director, National Security will maintain responsibility for ensuring that all SAP Cadre agents are trained to this standard.

2.10.e. SAP Cadre Security Clearances. All SAP Cadre special agents will be required to obtain and maintain TS/SCI with access to the following control systems: SI, TK, G, and HCS.

2.10.f. SAP Investigations by Non-SAP Cadre: Upon request of a Field Office SAC, and with the approval of the Program Director, National Security, non-SAP Cadre agents may work SAP investigations under the following circumstances:

2.10.f.(1). The special agent possesses the requisite security clearance.

2.10.f.(2). The special agent has successfully completed all required SAP Cadre training.

2.10.f.(3). The SAC, OSEC, and Program Manager, Classified Investigations have coordinated with SAPCO to obtain for the special agent access to a SAP-F, adequate storage, and adequate data processing resources for the SAP.

2.11. SCI Eligibility and Access

2.11.a. Requesting SCI Eligibility. All DCIS special agents hold TS security clearances. The process used to upgrade an agent's clearance from Top Secret to "Top Secret - SCI Eligible" involves a personnel action called a "Position Sensitivity Upgrade" followed by an adjudication decision by DIA. The process begins with a memorandum justifying the operational need to upgrade an individual's clearance. This unclassified memo, entitled "Request for SCI Upgrade," is initiated by the agent's supervisor and submitted to the DoD IG Special Security Representative (SSR) for routing. The DIA is the DoD IG's executive agency for adjudicating SCI eligibility requests.

2.11.b. Requesting SCI Access. This is the process used to change an agent's status from "SCI Eligible" to "SCI Access". The decision to grant SCI access is driven by the need for access to SCI information or assignment to duties/missions that require access to SCI—essentially a need to know. Individuals who are not assigned to missions that require SCI access or to perform duties at that level are kept in the "SCI Eligible" status until the need for SCI arises. The process to change an agent's status requires submission of a memo titled "Justification/Request for Sensitive Compartmented Information (SCI) Access." The Justification/Request for SCI is required to validate the individual's need to know, mission, and specific program accesses required. It is also used to coordinate the SCI indoctrination with the Special Security Officer (SSO) for the SCIF where the duties will be performed. In accordance with guidance from the DoD IG SSO, this memo template is UNCLASSIFIED, but should be

treated as CONFIDENTIAL when filled in because it identifies the location of a SCIF. While the locations of all SCIFs are not necessarily classified, many are. Treating the memo as CONFIDENTIAL precludes any spillage of potentially classified information to non-classified systems. The memo should be drafted, processed and submitted to the DoD IG SSR via SIPRNET for routing. For offices without SIPRNET, contact the Program Manager, Classified Investigations for assistance.

2.12. Passing Security Clearances

2.12.a. Passing SECRET clearances. A DCIS supervisor should forward a DCIS Form 12, Defense Criminal Investigative Service Visit Request, (Attachment A) to the Office of Security at personnel_security@dodig.mil. The Office of Security will notify the DCIS supervisor by email when the clearance has been passed to the appropriate facility.

2.12.b. Passing TS/SCI Clearances. A DCIS supervisor should forward a DIA Form 128 to the DoD IG SSR. The SSR will notify the DCIS supervisor by email when the clearance has been passed to the appropriate facility. Contact the Program Manager for Sensitive Investigations to obtain the most recent version of the DIA Form 128.

2.12.c. Accurate Information. Inaccurate information on the DCIS Form 12 or the DIA Form 128 will hinder the passing of the clearance. Before sending any request to pass a clearance, ensure all points of contact and associated contact information are accurate. When requesting your clearance to be passed to the FBI, ensure your point of contact is an FBI employee and not a contractor. Requests listing an FBI contractor as a POC will be disapproved.

2.12.d. Encryption. Both the DCIS Form 12 and the DIA Form 128 contain Personally Identifiable Information when properly completed. When submitting these forms to the Office of Security or the SSR, ensure your email is encrypted.

2.13. Access to SAPs

2.13.a. Requesting Access to a SAP. Agents with a need to access a SAP should submit the request through their supervisor to the Program Manager, Classified Investigations. To initiate the request, the supervisor should call the Program Manager, Classified Investigations with the names of those requiring access as well as the unclassified nicknames of the SAP(s). The Program Manager will coordinate the request with the SSR, SSO, Intelligence and Special Programs Assessment (ISPA) and the DoD SAPCO. The SSO or ISPA will advise the agents requesting access of any further requirements. The SSO will advise the Program Manager, Classified Investigations, when an agent is approved for access, and will provide instructions for the agent to get “read on”, or accessed, to the SAP. To be accessed to a DoD SAP, the candidate must:

2.13.a.(1). Be nominated for access.

2.13.a.(2). Possess a final TOP SECRET or SECRET security clearance.

2.13.a.(3). Have a current investigation validated by the DoD SAPCO.

2.14. **Courier Cards**

2.14.a. **Secret Courier Cards.** A courier card is required before any DCIS agent can transport Secret material. Contact the DoD IG Office of Security to obtain a Secret courier card.

2.14.b. **Top Secret or TS/SCI Courier Cards.** Coordinate requests to courier Top Secret or TS/SCI material through the Program Manager, Sensitive Investigations and the DoD IG Special Security Officer (SSO).

ATTACHMENT A

DEFENSE CRIMINAL INVESTIGATIVE SERVICE VISIT REQUEST

All fields must be completed

If passing TS/Collateral and below send form to Personnel_Security@DODIG.MIL

If passing TS/SCI use DIA Form 128 and send to the Office of Security, Special Security Representative

PRIVACY ACT STATEMENT

Authority: DoD 5200.2-R, DoD Personnel Security Program Regulation; and E.O. 9397 (SSN)

Purpose: This information is requested in order to verify need for access to facility, and if necessary, classified information.

Routine Use: Information on the clearance/eligibility status of individuals may be provided to the appropriate clearance access officials of other agencies when necessary in the course of official business. Certifications of clearance are issued to officials of other agencies when necessary in the course of official business.

Disclosure: Voluntary, however, failure to provide the requested information may result in denial of access to facilities and information.

SECTION I - DESTINATION INFORMATION

1. NAME OF ORGANIZATION YOU PLAN TO VISIT:

2. LOCATION: *(Please include City, State)*

3. INITIAL VISIT DATE: *"Permanent Cert may be up to 1 year"*

THRU:

4. REASON FOR VISIT: *"Please be specific but must be unclassified"*

5. CLEARANCE/ACCESS (ES) REQUIRED: (Check One) ☐ SECRET ☐ TOP SECRET

6. POC NAME: *"List the Technical POC for the facility you are visiting - not the Security POC"*

7. POC PHONE:

8. POC E-MAIL:

9. SECURITY POC NAME:

10. SECURITY POC PHONE:

12. SECURITY POC E-MAIL:

11. SECURITY POC FAX NUMBER(S):

13. SMO CODE *(If known)*

SECTION II - VISITOR(S) INFORMATION

14. NAME:

15. GS LEVEL:

16. SOCIAL SECURITY #:

17. PHONE NUMBER:

18. DATE OF BIRTH:

19. NAME:

20. GS LEVEL:

21. SOCIAL SECURITY #:

22. PHONE NUMBER:

23. DATE OF BIRTH:

24. NAME:

25. GS LEVEL:

26. SOCIAL SECURITY #:

27. PHONE NUMBER:

28. DATE OF BIRTH:



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

May 19, 2016

MEMORANDUM FOR ALL DCIS SPECIAL AGENTS

SUBJECT: Interim Policy for Special Agents Manual (SAM) Chapter 2, "Sensitive Investigations Program," regarding Revised Instructions for Passing Security Clearances

Effective immediately, this interim policy rescinds the requirement found in SAM Chapter 2 to use Attachment A, DCIS Form 12, Defense Criminal Investigative Service Visit Request, to pass collateral security clearances for DCIS employees. The DCIS Form 12 is hereby removed from Chapter 2 and will no longer be utilized. The DCIS Form 12 has been replaced with a form generated by the OIG Office of Security.

Effective immediately, this interim policy updates SAM Chapter 2, paragraph 2.12 to read as follows.

2.12. Passing Security Clearances

2.12.a. Passing SECRET or TOP SECRET (Non-SCI) Clearances. DCIS employee clearances can only be verified and passed by the OIG's Office of Security (OSEC). All employees who require a clearance to be passed must complete OSEC's Visit Request Form prior to visiting an outside agency/facility or contractor site. The form can be found on OSEC's homepage: <https://intra.dodig.mil/MST/Security/pdfs/OfficeofSecurityUpdateVisitRequestForm.pdf>. Upon completion, the form should be forwarded to OSEC via Personnelsecurityactions@dodig.mil. OSEC will notify the employee by email when the clearance has been passed to the appropriate facility.

2.12.b. Passing TS/SCI Clearances. DCIS employees accessed to SCI who require their SCI clearance to be passed or verified must submit DIA Form 128 to the DoD OIG Special Security Representative (SSR) or the DCIS Sensitive Investigations Program Manager (PM) for coordination. All SCI visit requests require 5 business days lead-time for processing by the OIG Special Security Officer (SSO). The SSR or SSO will notify the employee once the clearance has been passed to the appropriate facility.

2.12.c. Accurate Information. Inaccurate information on the DIA Form 128 will hinder the passing of the clearance. Before

sending any request to pass a clearance, ensure all points of contact and associated contact information are accurate. When requesting your clearance to be passed to the FBI, ensure your point of contact is an FBI employee and not a contractor. Requests listing a FBI contractor as a POC will be disapproved.

2.12.d. **Encryption.** The DIA Form 128 and any other visit request correspondence containing Personally Identifiable Information should be encrypted when emailed.

This policy is in effect until it is rescinded or incorporated into the next revision of SAM Chapter 2. Any questions related to this policy should be directed to (b)(6), (b)(7)(C) Deputy Assistant Inspector General for Investigations, Investigative Operations Directorate, at 703-604-(b)(6), (b)(7)(C)

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

Deputy Assistant Inspector General
for Investigations

CHAPTER 3

ASSET FORFEITURE PROGRAM

<u>Contents</u>	<u>Section</u>
General	3.1.
Definitions	3.2.
Theories and Types of Forfeiture	3.3.
Asset Forfeiture Programs	3.4.
DCIS Asset Forfeiture Program	3.5.
Operational Instructions	3.6.
Asset Forfeiture Input Into IDS	3.7.
Forfeiture Procedures	3.8.
Official Use of Forfeited Assets	3.9.
Seizure	3.10.
Inventory, Appraisal, and Custody of Seized Property	3.11.
Remission and Restoration	3.12.

3.1. General. This chapter outlines policies, procedures, and restrictions governing the Defense Criminal Investigative Service (DCIS) Asset Forfeiture Program (AFP) and its participation in the United States Department of Justice (DOJ) Asset Forfeiture Program.

3.1.a. DCIS is a full participating member in the United States Department of Justice Asset Forfeiture Fund (DOJ-AFF).

3.1.b. Members of the DOJ-AFF are identified in paragraph 3.7.a. In contrast, the Department of Treasury has established its own forfeiture program, which is unrelated to the DOJ-AFF. Participants in the Treasury fund are also identified in paragraph 3.7.b.

3.1.c. The DCIS-AFP will be centralized within Investigative Operations and the Program Director will report to the Special Agent in Charge (SAC), Investigative Operations. The DCIS-AFP is responsible for coordinating and maintaining all contact with the DOJ-AFP.

3.2. Definitions

3.2.a. **Administrative Forfeiture.** Administrative forfeiture is a process by which property may be forfeited to the United States without judicial involvement by the investigative agency that seized it. **Please note: DCIS does not have administrative forfeiture authority.**

3.2.b. **Civil Forfeiture (*in rem*).** Civil forfeiture is not part of a criminal case. In a civil forfeiture case, the Government files a separate civil action *in rem* against the property itself, and then proves, by a preponderance of the evidence, that the property was derived from or was used to commit a crime.

3.2.c. **Criminal Forfeiture (*in personam*)**. Criminal forfeiture requires a defendant be charged and convicted of a crime directly related to property obtained as a result of the crime and is sought after the conviction. Criminal forfeiture is part of the sentence of a convicted criminal. Therefore, the defendant's property cannot be criminally forfeited if the defendant dies before being convicted, is a fugitive, or is acquitted.

3.2.d. **Forfeiture**. The divestiture of property without compensation. The loss of a right, privilege, or property because of a crime, breach of obligation, or neglect of duty. Forfeited property may include not only offending items such as conveyances, but other property that is traceable to the proceeds from the commission of the offense or property that was used to facilitate the offense.

3.2.e. **Proceeds**. Whatever is received when an object is sold, exchanged, or otherwise disposed.

3.2.f. **Exclusionary Rule**. The rule in a criminal trial that prevents the admission of evidence obtained in violation of a person's U.S. constitutional rights.

3.2.g. **Victim**. A person who has suffered a specific pecuniary loss as a direct result of the crime underlying the forfeiture or a related offense. The definition of "person" includes "an individual, partnership, corporation, joint business enterprise, estate, or other legal entity capable of owning property." See Title 28, Code of Federal Regulations (CFR) 9.2.(m).

3.3. Theories and Types of Forfeiture

3.3.a. **Jurisdictional Theories**. There are two broad jurisdictional theories of forfeiture:

- 3.3.a.(1). *In personam* (criminal forfeiture).
- 3.3.a.(2). *In rem* (civil forfeiture).

3.3.b. **Forfeiture Provisions**. There are three types of forfeiture provisions:

- 3.3.b.(1). Administrative
- 3.3.b.(2). Civil Judicial
- 3.3.b.(3). Criminal Judicial

3.3.c. **Administrative Forfeiture**

3.3.c.(1). DCIS does **not** have administrative forfeiture authority.

3.3.c.(2). Federal agencies with administrative forfeiture authority:

- 3.3.c.(2).(a). Federal Bureau of Investigation (FBI)
- 3.3.c.(2).(b). Drug Enforcement Administration (DEA)
- 3.3.c.(2).(c). Bureau of Immigration and Customs Enforcement (ICE)
- 3.3.c.(2).(d). Internal Revenue Service (IRS)

- 3.3.c.(2).(e). U.S. Postal Inspection Service (USPIS)
- 3.3.c.(2).(f). U.S. Secret Service (USSS)
- 3.3.c.(2).(g). Alcohol, Tobacco, Firearms, and Explosives (ATFE)

3.3.d. **Civil Forfeiture.** Property can be civilly forfeited even if its owner is never called to defend against criminal charges or, if charged, dies, becomes a fugitive, or is acquitted. The legal fiction is that the property is guilty and the action is against the property, rather than a named person. Civil forfeiture requires a lower standard of proof, preponderance of the evidence, in contrast to criminal forfeiture, which requires beyond a reasonable doubt.

3.3.e. **Criminal Forfeiture.** A criminal forfeiture action is also judicial and requires that a Federal grand jury return an indictment against an individual or the individual must agree to plea to an information filed by an Assistant U.S. Attorney. Included in the indictment or information is a count charging that the property belonging to the defendant is subject to forfeiture.

3.4. Asset Forfeiture Programs

3.4.a. **The Department of Justice (DOJ) Asset Forfeiture Program.** The Defense Criminal Investigative Service's AFP is a part of the Department of Justice Asset Forfeiture Program. This program includes the following member agencies:

- 3.4.a.(1). DOJ's Asset Forfeiture Management Staff
- 3.4.a.(2). DOJ's Asset Forfeiture/Money Laundering Section
- 3.4.a.(3). DOJ's Executive Office for U.S. Attorneys
- 3.4.a.(4). Assistant United States Attorneys
- 3.4.a.(5). United States Marshals Service (USMS)
- 3.4.a.(6). Drug Enforcement Administration (DEA)
- 3.4.a.(7). Federal Bureau of Investigation (FBI)
- 3.4.a.(8). U.S. Postal Inspection Service (USPIS)
- 3.4.a.(9). Food and Drug Administration (FDA)
- 3.4.a.(10). U.S. Park Police
- 3.4.a.(11). U.S. Department of Agriculture (USDA)
- 3.4.a.(12). Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATFE)
- 3.4.a.(13). Department of State, Diplomatic Security Service (DSS)

DCIS deposits forfeited cash and proceeds from the sale of forfeited property into this fund.

3.4.b. **The Department of Treasury Asset Forfeiture Program.** The Department of Treasury established its own forfeiture program, which operates independently from the Department of Justice. Although the Department of Treasury created a separate forfeiture fund, the program operation is nearly identical to the Department of Justice Forfeiture Program. Members of the Department of Treasury Forfeiture Program include:

- 3.4.b.(1). Bureau of Immigration and Customs Enforcement (ICE)
- 3.4.b.(2). Department of Homeland Security (DHS)

- 3.4.b.(3). U.S. Secret Service (USSS)
- 3.4.b.(4). Internal Revenue Service (IRS)
- 3.4.b.(5). U.S. Customs and Border Protection (CBP)

The Department of Treasury's seizing agencies deposit forfeited cash and proceeds from the sale of forfeited property into this fund.

3.4.c. The United States Postal Inspection Service (USPIS) Forfeiture Fund.

Although the USPIS is part of the DOJ-AFF, it is unique in that it has its own forfeiture fund program. Specifically, forfeited cash and proceeds from the sale of property administratively forfeited by the Postal Inspection Service are deposited into the Agency forfeiture fund. Additionally, the Postal Inspection Service's share of judicially forfeited cash and proceeds from the sale of judicially forfeited property is also deposited into this fund.

3.5. DCIS Asset Forfeiture Program

3.5.a. **Goals.** The DCIS AFP has three primary goals:

3.5.a.(1). to punish and deter criminal activity by depriving criminals of property used or acquired through illegal activities;

3.5.a.(2). to enhance cooperation among foreign, Federal, state, and local law enforcement agencies through the equitable sharing of assets recovered through this program and; as a by-product,

3.5.a.(3). to produce revenues to enhance forfeitures and strengthen law enforcement.

3.5.b. DCIS AFP Structure

3.5.b.(1). The AFP consists of a DCIS Special Agent who is the Program Director (PD) (full time equivalent (FTE)) supported by four Headquarters contractors: a Project Director (PJD) and three staff auditors. Additionally, there are 12 contract investigators assigned to the 6 field offices and additional full-time and part-time subcontractors providing forensic accounting and telephonic analysis support.

3.5.b.(2). The Program Director (PD) is responsible for managing the entire program and its growth and is the approval authority for all purchases, travel, equitable and reverse sharing requests, and the budget. Further, the PD is responsible for all interactions with the Department of Justice, Asset Forfeiture & Money Laundering Section (AFMLS), and the Asset Forfeiture Management Staff (AFMS).

3.5.b.(3). The Project Director (PJD) is responsible for, under the direction of the PD, overseeing and managing the field contractors and providing subject matter guidance.

3.5.b.(4). The staff auditors are responsible for maintaining the Consolidated Asset Tracking System (CATS), preparing Financial Crimes Enforcement Network (FinCEN) Intel reports, conducting database queries, and preparing monthly budget reports.

3.5.c. **Responsibilities.** The AFP is responsible for the development of procedures and policy, program management, program oversight, training, budget, and strategic planning for all of DCIS's asset forfeiture initiatives. Specifically, the AFP is responsible for:

3.5.c.(1). Developing policies and procedures based on legislative changes, DOJ guidelines, and relevant Federal court decisions.

3.5.c.(2). Overseeing DCIS asset forfeiture efforts, including a comprehensive review of all investigations prior to pursuing forfeiture, including seizing and disposal of forfeited property.

3.5.c.(3). Coordinating and maintaining an ongoing working relationship with the Department of Justice Asset Forfeiture Program, to include AFMS and AFMLS.

3.5.c.(4). Continually interacting with field office personnel regarding forfeiture matters. The Asset Forfeiture Program provides support with difficult and unique seizures and forfeitures.

3.5.c.(5). Providing all forfeiture-related training directly or through AFMS sanctioned training venues. Forfeiture funds will be used to pay for the training.

3.5.c.(6). Tracking all funds seized for forfeiture, which includes fund transfers from USMS holding accounts to fund revenue accounts.

3.5.c.(7). Approving, coordinating, monitoring, and managing all asset forfeiture-related purchases and expenses to include, but not limited to, equipping of conveyances (lights, sirens, radios, and tinting), purchasing ADP equipment, case-related expenses, items, awards, contracts to identify assets, and asset management and disposal.

3.5.c.(8). Approving and coordinating forfeiture investigative support (forensic accounting and telephonic/e-mail/scanning analysis) once notified by the case agent of an investigation in which forfeiture will be sought (see section 3.6., Operational Instructions).

3.5.c.(9). Approving and monitoring all case agent and contract investigator AFP-related travel.

3.5.c.(10). Providing all CATS asset support.

3.5.c.(11). Coordinating with Treasury Department Asset Forfeiture fund agencies in regard to reverse sharing.

3.5.c.(12). Coordinating with state and local law enforcement agencies in regard to equitable sharing.

3.5.d. **Contract Investigators.** Contract investigators assigned to each field office are responsible for, but not limited to, the following:

3.5.d.(1). Reviewing all open cases and determining which investigations have AF potential.

3.5.d.(2). Coordinating with case agents the forfeiture part of the general investigative activity.

3.5.d.(3). Accompanying case agents to forfeiture-related meetings at the United States Attorneys Office (USAO) and/or making presentations.

3.5.d.(4). Preparing mail covers and FinCEN requests (based on biographical information provided by the case agent).

3.5.d.(5). Reviewing and briefing to the case agent all contractor forensic accounting and telephonic support investigative reports.

3.5.d.(6). Assisting case agents in preparing and reviewing affidavits in support of temporary restraining orders and seizure warrants.

3.5.d.(7). Assisting agents in preparing and reviewing the forfeiture portion of indictments, informations, and plea agreements.

3.5.d.(8). Notifying the AFP, for tracking purposes, when an administrative forfeiture is being conducted on a DCIS investigation and the agency supporting the administrative forfeiture.

3.5.d.(9). Reviewing and maintaining a copy of all Federal Contribution Forms completed by case agents or Treasury Asset Forfeiture Fund participating agencies prior to submission to the AFP for review and signature.

3.5.d.(10). Coordinating asset appraisals with the case agent.

3.5.d.(11). Coordinating pre-seizure planning with the case agent and the appropriate United States District office.

3.5.e. **Case Agent Responsibilities**

3.5.e.(1). The case agent is responsible for conducting all general investigative activity on any case that has been identified as a forfeiture-related investigation.

3.5.e.(2). The agent will coordinate with the prosecuting AUSA to add the contract investigator(s) to any existing 6(e) lists.

3.5.e.(3). The case agent will identify for the contract investigator the name, date of birth (DOB), address, and Social Security number (SSN) for which mail covers and FinCENs will be prepared by the contract investigator.

3.5.e.(4). The case agent will provide investigative facts and evidence to assist the contract investigator in preparing affidavits in support of seizure warrants and temporary restraining orders for property designated for forfeiture.

3.5.e.(5). When speaking with the AFP regarding AF-related travel requests, purchases, or contract support, the case agent will adhere to instructions provided under section 3.6., Operational Instructions.

3.5.e.(6). The case agent will coordinate with the contract investigator and the AFP on all seizures for forfeiture. The AFP will provide the case agent a CATS number for the items to be seized for forfeiture. Please Note: The USMS will not accept any property that does not have an assigned CATS number.

3.5.e.(7). The case agent, with assistance from the contract investigator and the AFP, will recommend an appropriate percentage of equitable sharing with state and local law enforcement agencies based on their direct participation in the investigation. The final determination for equitable sharing with foreign law enforcement agencies that have assisted on a forfeiture investigation is made by AFMLS or the Deputy Attorney General in consultation with the Department of State.

3.5.e.(8). The case agent, with assistance from the contract investigator and the AFP, prepares the Federal Contribution Form (FCF) when DCIS is not the lead on the forfeiture and the joint Agency participates in the Treasury Asset Forfeiture Fund.

3.5.e.(9). The case agent reviews, with assistance from the contract investigator, all FCFs submitted by Treasury Asset Forfeiture Fund participating agencies that were jointly investigating a case in which DCIS is the forfeiture lead. The case agent and the contract investigator will forward the FCF request to the AFP.

3.5.f. Special Agent in Charge

3.5.f.(1). **Official Use Requests.** The Special Agent in Charge (SAC) requests permission to retain forfeited property for official use (see Official Use Policy).

3.5.f.(2). **Program Oversight.** The SAC (can be delegated to Assistant Special Agent in Charge/Resident Agent in Charge (ASAC/RAC)) plays a major role in monitoring whether offices are effectively and efficiently using forfeiture as a tool in investigations.

3.5.f.(3). **SAC Responsibility.** The SAC is responsible (can be delegated to the ASAC/RACs) for reviewing and signing contract investigator travel vouchers and assigning/coordinating contract investigator workload. Please note that case agent and contract investigator asset forfeiture-related travel must be pre-approved by the PD.

3.6. Operational Instructions

3.6.a. Asset Forfeiture Purchase Requests

STEP 1:

The case agent and/or the agent's direct supervisor must submit an e-mail to the PD, Asset Forfeiture, requesting approval to purchase an item or service (e.g., asset appraisal) using a local Government Purchase Card (GPC) for reimbursement using asset forfeiture funds.

The e-mail must include a brief justification (include case name and Case Control Number (CCN)) describing the purpose and need for the asset forfeiture-related purchase. If the agent prepares the request, then the agent's direct supervisor must be cc'd and vice versa. The AFP Project Director (PJD) and staff auditors (AUDs) must be cc'd on the e-mail request.

STEP 2:

If the request is approved, the PD will notify the case agent and direct supervisor via e-mail.

STEP 3:

The local administrative officer will pull the monthly GPC billing statement on the 20th of the month in which the purchase appears and highlight the purchase.

STEP 4:

The highlighted billing statement and all supporting documents (invoices, estimates, FedEx paperwork, approving e-mail, etc.) need to be forwarded by the administrative officer to the appropriate Program Analyst, Budget and Personnel, Headquarters, by the 21st of that month. The PD, PJD, and AUDs in Step 1 must be cc'd on the e-mail. All supporting documents including the bill must be marked with the office code, CCN#, and the phrase "Asset Forfeiture Fund." If the purchase involved the equipping of a Government Owned Vehicle (GOV), then the G-tag (in place of the CCN#), office code, and the phrase "Asset Forfeiture Fund" will be noted on all documents.

3.6.b. Asset Forfeiture Travel Requests

STEP 1:

The case agent and/or the agent's direct supervisor must submit an e-mail request for travel to the PD, Asset Forfeiture.

The e-mail must provide a brief justification (include case name and CCN) describing the asset forfeiture-related purpose of the travel.

If the agent prepares the request, then the agent's direct supervisor and field office management must be cc'd and vice versa. The AFP PJD and AUDs must be cc'd on the e-mail.

STEP 2:

If the request is approved, the PD will notify the case agent, direct supervisor, and office management via e-mail.

STEP 3:

The case agent will prepare and sign a travel authorization in Defense Travel System (DTS) using the AST FRFTR line of accounting (LOA) and e-mail the PD and AUDs the trip cost and "TA Number."*. The PD will then request the DTS Program Analyst, Budget and Personnel, Headquarters, to fund the appropriate LOA.

Please Note: All asset forfeiture travel must follow Government travel requirements and restrictions regarding rental cars, per diem, lodging rates, etc.

* Once the authorization is signed and approved the "TA Number" can be obtained by clicking on the "Official Travel" tab, then click on the "Authorization/Orders" tab, locate the authorization under the "Sort by Document Name" and report the six-digit TA Number in the fourth column titled "Sort by TA Number." Examples of TA Numbers would be "140T14," "115451," "0UG19K" etc.

3.6.c. Contract Forfeiture Requests (Forensic Accounting, Telephonic/E-mail/Scan Support)

STEP 1:

The case agent and the contract investigator should contact (b)(6), (b)(7)(C) and/or (b)(6), (b)(7)(C) to discuss the elements of the case.

STEP 2:

If the initial discussion identifies areas in which forensic accounting and/or telephonic contract support could be useful in the further identification of assets, then the case agent and/or the agent's direct supervisor must submit an e-mail requesting investigative support to the PD, AFP. The e-mail must include a brief justification (include case name and CCN) for the support requested. If the agent prepares the request, then the agent's direct supervisor should be cc'd and vice versa. The PJD and AUDs must be cc'd on the e-mail.

STEP 3:

If the request is approved, the PD will notify the case agent, direct supervisor, and contract support via e-mail.

Contact Information:

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

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

3.6.d. **Scanning-OCR Instructions.** Scanning/imaging and Optical Character Recognition (OCR) contract forfeiture support is available during the execution of search warrants in support of investigations involving forfeiture. Instructions for requesting such support are listed below:

STEP 1:

The case agent and/or the case agent's direct supervisor must submit an e-mail requesting scanning/imaging and OCR support to the PD, Asset Forfeiture. If the agent prepares the request, then the agent's direct supervisor and field office management must be cc'd and vice versa. The AFP PJD and AUDs must be cc'd on the e-mail. The e-mail must include a justification that includes the following information:

3.6.d.(1). case name and CCN;

3.6.d.(2). the statute(s) that allows for forfeiture;

3.6.d.(3). the statement, "Prosecuting attorney will pursue forfeiture if the evidence warrants";

3.6.d.(4). identify (include phone numbers) the prosecuting AUSA and forfeiture AUSA assigned to the investigation;

3.6.d.(5). a document that the contract forfeiture investigator assigned to the investigation concurs with the request;

3.6.d.(6). document coordination with NTI (Bob Lottero) and Nossen & Associates (Wendy Spaulding) regarding forensic accounting and/or telephonic and e-mail analysis of OCR evidence;

3.6.d.(7). confirm the potential forfeiture covers at a minimum the cost of the estimated work requested.

STEP 2:

If the request is approved, the PD will notify the case agent, direct supervisor, and field office management via e-mail.

Contact Information:

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

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

3.7. Asset Forfeiture Input Into IDS

(b)(7)(E)

(b)(7)(E)

3.8. Forfeiture Procedures

3.8.a. Forfeiture Procedures Outline

Civil Forfeiture Steps	Criminal Forfeiture Steps
Pre-seizure Planning	Indictment
Seizure via seizure warrant	Seizure via Seizure Warrant
Custody and Appraisal	Seizure via Preliminary Forfeiture Order
Notice	Consent Order of Forfeiture (if a plea/information is obtained)
Claims	Custody and Appraisal
Petitions for Remission	Notice
Disposition	Trial & Conviction
	Ancillary Hearing
	Final Order of Forfeiture
	Petitions
	Disposition

3.8.b. Pre-Seizure

3.8.b.(1). Pre-seizure is the establishing of a plan for the seizure of property for forfeiture and requires considering law enforcement responsibility, economic realities, and the rights of innocent parties. Also, one must consider the impact on the entire criminal case in making the decision to seize property for forfeiture.

3.8.b.(2). The decision regarding whether to seize property for forfeiture usually involves consultation with an Assistant U.S Attorney (AUSA), and later on with the USMS.

3.8.b.(3). DCIS discourages the seizure of certain types of property, including:

(b)(7)(E)

(b)(7)(E)

3.8.b.(4). Please recognize that seizures are made regardless of the costs to the Government and for a law enforcement benefit. However, since forfeiture is punitive in nature, the value of property should be proportional to the seriousness of the offense.

3.8.c. **Minimum Monetary Thresholds**

3.8.c.(1). Use these thresholds as a guide to assist in determining whether assets should be seized for forfeiture. Exceptions to this policy will be considered; however, there must be a significant law enforcement benefit obtained through forfeiture. NOTE: (b)(7)(E)

(b)(7)(E) The equity is the value of the property after subtracting the anticipated cost of forfeiture and claims of innocent owners from the appraised value.

3.8.c.(2). Property categories and minimum monetary thresholds for DCIS are as follows:

Vehicles
Vessels
Aircraft
Real Property

(b)(7)(E)

Cash (Includes bank accounts and monetary instruments)	(b)(7)(E)
Other Property	
Weapons	No Minimum Value
Visual Depictions (Child Exploitation)	No Minimum Value

* Vehicles worth \$75,000 or more are considered luxury conveyances and will generally not be placed into official use (exemptions will be considered); however, they are still eligible for forfeiture.

3.8.d. Exceptions to Minimum Monetary Thresholds. All other property types must meet the existing monetary thresholds for property type unless a minimum threshold deviation is obtained. Whenever possible, DCIS should encourage inclusion of such property in the criminal indictment.

3.8.e. Minimum Threshold Deviation. Deviation from minimum threshold request must be submitted to the PD whenever the following exists:



(b)(7)(E)

To request a deviation from the minimum monetary threshold, the SAC must submit a memorandum to the PD requesting waiver and describing the significant law enforcement benefit obtained through the forfeiture. The deviation request must be submitted immediately after seizure. (Note: There will be times when the minimum threshold is not known; however, all attempts should be made to determine it prior to seizure.) The deviation request should include a description of the property, the appraised value, the facts and circumstances surrounding the seizure, and the law enforcement justification for the forfeiture. If a law enforcement objective is served by the forfeiture of property with a minimal value, the forfeiture will be granted by the PD through an e-mail. If a law enforcement objective is not clearly defined, or the costs of the forfeiture significantly outweigh the benefits, the PD will deny the deviation request.

3.9. Official Use of Forfeited Assets

3.9.a. Summary

3.9.a.(1). When it is in the best interest of the Agency, DCIS may request seized vehicles be placed into official use. A memorandum from the field SAC to the SAC, Investigative Operations, through the PD must be submitted. The SAC, Investigative Operations is the approving official for all requests to place forfeited property into official use.

3.9.a.(2). In terms of vehicles, the following must be considered:

3.9.a.(2).(a). In deciding whether to accept or decline a seized vehicle for official use, its total life-cycle cost will be considered. Operational utility and desirability must be balanced against the higher maintenance costs, which can be expected with these vehicles. Forfeited vehicles placed into official use should have a reasonable service life expectancy of at least 2 years.

3.9.a.(2).(b). A vehicle with no liens is preferable; however, asset forfeiture funds are available for lien payments up to 1/3 of the loan value. The vehicle must have at least \$10,000 equity value (all forfeited property for official use must meet the minimum monetary threshold, see paragraphs 3.8.c. through 3.8.e.) and no more than 50,000 miles. If a minimum monetary threshold waiver is necessary, the matter should be addressed in the memorandum requesting the asset be put into official use.

3.9.a.(2).(c). Any forfeited vehicle valued less than \$75,000 (Blue Book) can be used for undercover operations and/or general investigative activity. In contrast, high-end luxury vehicles valued in excess of \$75,000 will not be placed into official use (but will still be forfeited).

3.9.b. Seizure, Forfeiture, and Release

3.9.b.(1). Pre-seizure planning coordination with the USMS must take place days prior to the execution of a seizure warrant. Once a vehicle is seized for the purpose of placing it into official use, it will be towed to a mechanic for inspection and then to the USMS storage facility. All costs associated with the seizure will be funded from the AFP. The seized vehicle will be stored and maintained by the USMS until the court enters a Final Order of Forfeiture or a forfeiture order is issued by a Federal agency with administrative forfeiture authority. The USMS will charge DCIS storage fees from the date DCIS identifies a vehicle to be held for official use until the date the order of forfeiture is finalized. Storage fees will be paid using asset forfeiture funds.

3.9.b.(2). Upon final forfeiture the USMS will release the vehicle to DCIS with a "Certificate to Obtain Title to a Vehicle." Registration of forfeited undercover vehicles, to include obtaining the Certificate to Obtain Title to a Vehicle, titling, and plates will be coordinated between the DCIS Headquarters Program Manager for Undercover Operations (UCO) and the local DCIS office receiving the vehicle. The UCO Program Manager will monitor and determine the distribution of forfeited UC vehicles based on operational needs.

3.9.b.(3). If the vehicle is for overt investigative operations, the AFP will coordinate with the field office receiving the vehicle to register the vehicle. The AFP will monitor and determine the distribution of forfeited vehicles for general investigative activity. Please note that at this time there is no routine plan to place forfeited vehicles into official use for general investigative activity.

3.9.b.(4). It will be the responsibility of each field office receiving a vehicle to obtain title and plates. Upon completion, a copy of the title and related records will be sent to the AFP.

3.9.c. Official Use Memorandum

3.9.c.(1). Field offices must coordinate with the PD to obtain and use any forfeited vehicle, and a memorandum requesting approval will be prepared by the field office clearly defining the intended use. Careful consideration will be given to the vehicle's value and its potential benefit to the United States for Federal law enforcement purposes. The memorandum will include, but not be limited to the following information:

3.9.c.(1).(a). Specific information on how the vehicle will be used.

3.9.c.(1).(b). If needed, minimum monetary threshold waiver (see paragraph 3.11.c.(2).)

3.9.c.(1).(c). If needed, maximum monetary threshold waiver (see paragraph 3.11.c.(2).)

3.9.c.(1).(d). Year, make, model, color, mileage, CATS number, vehicle identification number (VIN).

3.9.c.(1).(e). Estimated cost of equipping the vehicle for law enforcement purposes (if applicable).

3.9.c.(1).(f). All information regarding any liens or other encumbrances against the vehicle or a statement that the vehicle is free of liens.

3.9.c.(1).(g). Attach to the memorandum:

3.9.c.(1).(g).1. A copy of the seizure warrant and existing vehicle registration with correct 17-digit VIN.

3.9.c.(1).(g).2. A copy of the mechanic's evaluation report and estimate of cost to place the vehicle in service.

3.9.c.(1).(g).3. Any Consent, Preliminary, or Final Orders of Forfeiture referencing the vehicle (if available).

3.9.c.(1).(g).4. Photographs of the vehicle.

3.9.c.(1).(h). The memorandum will include the following statement, "Seized vehicles being placed into official use ***cannot be used*** until there is a final order of forfeiture issued by a Federal court or a forfeiture order issued by a Federal agency with administrative forfeiture authority and the USMS releases the vehicle to DCIS."

3.9.c.(2). The memorandum should be forwarded to the PD as quickly as possible once the vehicle is seized through the use of civil or criminal seizure warrants by DCIS. Once

the request is approved by the SAC, Investigative Operations, the memorandum will be forwarded to the appropriate USMS office and Headquarters will enter the appropriate official use notification into CATS.

3.9.d. Operational Considerations

3.9.d.(1). Forfeited vehicles for undercover (covert) operations will be maintained with Emergency & Extraordinary Funds in accordance with the provisions of SAM Chapter 10.

3.9.d.(2). Forfeited vehicles for overt investigative purposes will be maintained with operational funds. At this time no decision has been made to supplement field vehicles with forfeited vehicles.

3.9.d.(3). Once forfeited vehicles are placed into service, the vehicles are subject to the same policies and procedures as DCIS official vehicles (such as authorized versus unauthorized uses, maintenance of vehicle history files, etc.) as denoted in SAM Chapters 36 (Motor Vehicles), 10 (Emergency and Extraordinary Funds), and IG Instruction 4100.33, "Government Purchase Card Program," August 31, 2009.

3.9.d.(4). All forfeited vehicles placed into official use will be accounted for as Government property and will be tracked by the AFP and Budget and Personnel on an Excel spreadsheet. The disposal of forfeited vehicles will be tracked by AFP and coordinated with the appropriate field office and the Defense Logistics Agency, Defense Reutilization and Marketing Service.

3.9.d.(5). Overt and covert forfeited vehicles are self-insured by the Government. The Federal Tort Claims Act provides the exclusive remedy for claims against the United States resulting from negligent operation of motor vehicles by Government employees within the scope of their employment.

3.9.e. Official Use of Other Forfeited Property. DCIS may acquire other forfeited property for official use to further its mission. As with vehicles, assets may not be accepted or placed into operation without written approval of the SAC, Investigative Operations and the PD. The standards for official use of any forfeited property will mirror those used for vehicles. Careful consideration will be given to the value of the property and its potential benefit to the United States for Federal law enforcement purposes.

3.10. Seizure

3.10.a. Authority to Seize. Title 10 U.S.C. §1585a authorizes DCIS to execute and serve any warrant (e.g., seizure warrant) or other process issued under the authority of the United States and to make arrests without a warrant.

3.10.b. Method of Seizure. There are several allowable methods for seizing property for forfeiture. Each method depends on the type of forfeiture action, whether exigent

circumstances are present, and the facts and circumstances of the violation. Exigent circumstances include protecting an individual's life or safety, pursuit in seeking a fugitive, or preserving evidence from immediate destruction or removal.

3.10.c. Seizure Warrant

3.10.c.(1). Warrant of Arrest In Rem

3.10.c.(1).(a). In a civil judicial case, the Government may take possession of property with an arrest warrant in rem. The procedure for issuing an arrest warrant in rem is set forth in Supplemental Rule G(3).

3.10.c.(1).(b). Under the Rule, no arrest warrant is needed if the property is real property, or if the property is already subject to a pretrial restraining order. That is because in those cases, the court already has in rem jurisdiction over the property, making the arrest warrant in rem unnecessary for that purpose. In all other cases, however, the Government must obtain an arrest warrant in rem and serve it on the property to ensure that the court obtains in rem jurisdiction.

3.10.c.(2). **Seizure Warrant.** A second form of process for seizing forfeitable property is the warrant of seizure authorized by 21 U.S.C. §881(b) and 18 U.S.C. §981(b)(2). This form of process requires a judicial determination of probable cause.

3.10.c.(3). **Seizure of Real Property.** In general, real property is not seized prior to forfeiture, nor is it served with an arrest warrant in rem. Typically, a *lis pendens* is filed in the property records of the local jurisdiction. The procedures for commencing a civil forfeiture action against real property are set forth in 18 U.S.C. §985.

3.10.c.(4). **Defense Criminal Investigative Service Seized Property Custody Document (DCIS Form 16).** DCIS Form 16 will be used whenever a property custody document is needed for property seized for forfeiture. In contrast, DCIS Form 14 is used for custody of property that is seized for evidence. Please note that the United States Marshals Service will **NOT** accept evidence. If circumstances change in which property seized as evidence is now identified for forfeiture, a DCIS Form 16 will be completed and attached to the original DCIS Form 14.

3.10.d. Seizures for Criminal Forfeiture

3.10.d.(1). **Property Seized Pursuant to a Civil Seizure Warrant.** The seizure of property pursuant to a civil seizure warrant issued under 18 U.S.C. §981(b) provides a valid basis for the Government's physical possession of property pending the outcome of a criminal forfeiture proceeding. But this is so only as long as the civil forfeiture matter is pending. In the Civil Asset Forfeiture Reform Act (CAFRA) of 2000, Congress provided that if someone files a claim in an administrative forfeiture proceeding, the Government has 90 days in which to (1) commence a civil forfeiture action, (2) commence a criminal forfeiture action, or (3) return the

property. *See* 18 U.S.C. §983(a)(3)(B). It is perfectly appropriate for the Government to file both a civil action and a criminal action within the 90-day period, or to file a civil action within 90 days and file a criminal action later. In such cases, the civil seizure warrant provides a valid basis for the Government's continued possession of the property.

3.10.d.(2). Property Seized Without a Warrant Based on Probable Cause.

Under 18 U.S.C. §981(b), property may be seized for civil or administrative forfeiture without a warrant if there is probable cause for the seizure and an exception to the warrant requirement applies. If those conditions are satisfied, the Government may maintain physical possession of the property pursuant to the 18 U.S.C. §981(b) seizure during the pendency of a criminal forfeiture case to the same extent as it could if the property had been seized with a warrant. That is, as long as the civil or administrative forfeiture case is ongoing, the continued possession may be based on the civil seizure. But if the civil case is terminated or not filed within the statutory deadline, the Government will have to maintain physical possession pursuant to a criminal seizure warrant or pretrial restraining order.

3.10.d.(3). Property Seized for Evidence. The seizure of property for evidence provides an independent basis for the continued physical possession of property during the pendency of a criminal forfeiture proceeding as long as the evidentiary value of the property persists. Thus, if property is seized for evidence, it may be named in a criminal forfeiture proceeding and held by the Government without the need to obtain a criminal seizure warrant or pretrial restraining order. However, if the evidentiary value of the property evaporates, the Government must obtain a seizure warrant or restraining order to maintain custody of the property for the purpose of forfeiture.

3.10.d.(4). Property Obtained From the State for Adoptive Forfeiture

3.10.d.(4).(a). A Federal seizing agency may take custody of property from a state or local law enforcement agency for the purpose of administrative forfeiture. If, in such a case, someone files a claim contesting the forfeiture, the 90-day deadline provision in 18 U.S.C. §983(a)(3)(B) comes into play. Thus, the Government's obligations regarding the continued physical possession of the property during the pendency of a criminal forfeiture proceeding are the same as they would be if the property had been seized for the purpose of civil forfeiture by a Federal agency in the first instance.

3.10.d.(4).(b). Alternatively, the Government may take possession of property from a state agency without any intention of proceeding with administrative or civil judicial forfeiture, but rather with the intent to seek the forfeiture of the property in a criminal case. In that instance, CAFRA does not apply, but neither does the provision in 18 U.S.C. §981(b)(2)(c) creating an exemption from the warrant requirement in adoption cases. That provision applies only to civil forfeiture proceedings. Therefore, the Government may maintain custody of the property only if it has evidentiary value, or if it obtains a criminal seizure warrant or pretrial restraining order.

3.10.d.(5). Property Seized for Evidence. There are instances when seizures are obtained through other permissible methods that do not violate an individual's Fourth

Amendment rights. For example, a convicted felon, released on parole, may be subjected to searches by a parole officer without prior notice and at any time. These searches, if properly conducted, are permissible under the terms of a parole agreement. Consultation should be made with the AUSA for guidance in conducting searches and seizures without a warrant.

3.10.e. **Adoptions.** An adoptive seizure refers to the Federal adoption and forfeiture of assets seized in cases where 100 percent of the pre-seizure activity was performed by a state or local agency. If DCIS participates in *any* portion of the investigation or seizure, the forfeiture case is considered a joint investigation.

3.10.f. **Reverse Sharing (Federal Contribution Forms) (FCF)**

3.10.f.(1). When DCIS is conducting a joint investigation with a Federal agency that participates in the DOJ-AFF and DCIS is the lead on the forfeiture, the AFP will list the agency in CATS as a participating investigative agency. Consequently, the investigative agency will receive full credit for any assets DCIS forfeits.

3.10.f.(2). If DCIS is not the lead on the forfeiture and the other agency participates in the DOJ-AFF, the case agent and/or contract investigator simply needs to request the other agency to list DCIS as an investigative agency in CATS. Consequently, DCIS will receive full credit, along with the other agency, for any assets forfeited.

3.10.f.(3). When DCIS is conducting a joint investigation with a Federal agency that participates in the Treasury Asset Forfeiture Fund, and DCIS is not the lead on the forfeiture, DCIS will need to submit to the Federal agency a FCF for each seized asset requesting sharing.

3.10.f.(3).(a). The FCF needs to be submitted within 60 days from the date of the seizure of the asset. The FCF needs to be completed by the case agent and contract investigator.

3.10.f.(3).(b). The FCF is then submitted to the PD for review and signature. The PD will then keep a copy and forward the original to the Treasury Asset Forfeiture POC.

3.10.g. **Real Property Seizures**

3.10.g.(1). **Forfeiture Actions With Real Property.** All forfeiture actions regarding real property must be handled in a judicial forfeiture proceeding. Upon identifying real property that is subject to forfeiture, the case agent and the contract investigator should contact the USMS to coordinate pre-seizure planning for the property.

3.10.g.(2). **Title Search.** The forfeiture of real property requires special considerations and procedures. For instance, prior to seizure, a sufficient search of the title must be conducted to determine the legal description, owner of record, and whether or not there are any recorded liens against the property.

3.10.g.(3). **Privacy Issues.** The seizure of real property that has an occupied structure involves heightened expectations of privacy. For instance, the authority to seize a residence is not sufficient to authorize entry or a custodial inventory search of the interior following the seizure. Where there is a privacy right protected by the Fourth Amendment, a search is reasonable only if there is a search warrant or other court order supported by probable cause or there exists an exception to the Fourth Amendment warrant requirement, such as consent or exigent circumstances.

3.10.g.(4). **Commercial Property.** The seizure of commercial property involves an assessment of factors other than just the value of real property. For instance, the seizure of commercial real property may significantly diminish the value of the property as an ongoing business. Early pre-seizure planning with the USMS is required.

3.10.g.(5). **Consultation.** Planning should include consultation with the AFP, the contract investigator, the U.S. Attorney's forfeiture AUSA, and the USMS.

3.10.h. **Other Seizing Considerations**

3.10.h.(1). **Timing of the Seizure.** Title 18 U.S.C. §983(a)(1)(A)(i) provides that notification in a non-judicial civil forfeiture should be sent as soon as practicable, and in no case more than 60 days after the date of seizure. Pre-seizure planning should include a strategy to ensure that there is enough time to initiate the civil forfeiture before the 60-day time frame expires. Initiation of forfeiture proceedings includes sending a civil administrative notice letter, filing a civil judicial complaint in rem against the property, or filing a criminal indictment against the defendant and listing the property in a forfeiture count. Please note that timing always depends on type of seizure.

3.10.h.(2). **Property Seized as Evidence.** See paragraph 3.10.d.(3).

3.10.h.(3). **Corresponding Criminal Prosecution.** If there is a corresponding criminal Federal prosecution, it may be more beneficial to delay seizure until a criminal indictment is filed against the defendant. The indictment should include a forfeiture count that specifically lists the property that is subject to forfeiture. Once the indictment is filed, assets can be seized or restrained pending the outcome of the criminal trial.

3.10.h.(4). **Sealing Search/Seizure Warrants.** On occasion, exigent circumstances may exist that make it advisable to have a search or seizure warrant and accompanying affidavits sealed. Unsealed warrants and accompanying affidavits become a matter of public record. If the case agent does not want to disclose the information contained in the warrant or the accompanying affidavits, the AUSA may file a motion with the district court to have the warrant and related paperwork sealed.

3.10.i. Preliminary Inquiries

3.10.i.(1). When possible, and prior to seizure, the case agent and/or the contract investigator must make preliminary inquiries to identify all parties who may have a potential interest in the seized property. These parties include:

- 3.10.i.(1).(a). Registered Owners
- 3.10.i.(1).(b). Other Owners
- 3.10.i.(1).(c). Spouses
- 3.10.i.(1).(d). Possessors
- 3.10.i.(1).(e). Lien-holders

3.10.i.(2). If an inquiry results in the identification of an innocent owner, it may not be beneficial for the Government to seize the property.

3.10.j. **Citing the Right to Financial Privacy Act.** Occasionally, lien-holders and other third parties who have an interest in the property seized for forfeiture are uncooperative in providing lien information. They believe the disclosure violates the Right to Financial Privacy Act. When lien-holders are uncooperative, refer to 12 U.S.C. §3403(d)(1), which permits the release of information incident to collecting on a debt.

3.11. Inventory, Appraisal, and Custody of Seized Property

3.11.a. **Inventory.** Before taking custody of assets seized for forfeiture, a complete and thorough inventory of the seized property must be conducted by the case agent and/or the contract investigator. A written receipt or warrant return should be provided to the person in possession of the property at the time of seizure.

3.11.b. Appraisal

3.11.b.(1). **Authority.** The contract investigator arranges for the appraisal of all property seized for forfeiture. The appraised value is the fair market value at the time and place of seizure.

3.11.b.(2). **Vehicle Appraisals.** For automobiles, trucks, recreational vehicles, and some boats, refer to the National Automobile Dealers Association (NADA) guide and use the average trade-in value at the time and place of seizure. The NADA guide is an online Internet subscription. Additional guides for specialty vehicles can also be accessed through the NADA online subscription at www.nada.com. The Vehicle Inventory Checklist must be completed to support the inventory of each seized vehicle. A copy of the appraisal page should be printed and, along with the Vehicle Inventory Checklist, filed in the official seizure file for documentation. If the vehicle is uncommon and no online guide is available, the contract investigator should request assistance from the USMS to secure a professional appraisal of the property. The NADA Guide subscription is for official business use only.

3.11.b.(3). **Electronic Equipment Appraisals.** Certain items, primarily electronic equipment, can be appraised by consulting the Orion Blue Book Web site. The Web site contains appraisals for computers, cameras, video equipment, televisions, and more. A password is not necessary to access the Web site. A copy of the appraisal page should be printed and used as documentation in the case file. The Orion Blue Book Web site subscription is for official business use only.

3.11.b.(4). **Jewelry Appraisals.** Since it is often difficult to determine if jewelry is genuine or costume, all jewelry should be professionally appraised. If evidence exists that the jewelry is costume, the senior investigator may have the jewelry reviewed by a jeweler to determine the approximate value. Otherwise, a professional appraiser should be used. Appraisal values and terminology differ nationally, so it is important to request that the appraiser provide the fair market value of the jewelry when the property is sold to the general public. The appraiser should work by the job, rather than by the value of the property items. The contract investigator should contact the USMS in the district to obtain appraisal recommendations.

3.11.b.(5). **Other Property Appraisals.** The value of other property, such as aircraft, art objects, and real estate must be professionally appraised. The appraiser should work by the job, rather than by the value of the property items. If possible, employ a member of a professional appraisers association or an appraiser used by other Federal agencies. The contract investigator should contact the USMS in the district to obtain appraisal recommendations.

3.11.b.(6). **Appraisals Involving Lien-Holders.** The contract investigator must determine the difference between the appraised value of the property at the time of seizure and the amount of monetary interest of the lien-holder or general creditor at the time of seizure. If this value does not meet or exceed the minimum monetary threshold, the asset should not be forfeited. For example, if a seized vehicle is appraised at \$15,000 with a lien of \$11,500, the \$3,500 difference between the appraised value and the monetary interest of the lien-holder is less than the minimum required monetary value of \$(b)(7)(E) established for vehicles. The seized vehicle should not be forfeited.

3.11.c. **Custody**

3.11.c.(1). **Authority.** Pursuant to 18 U.S.C. §981(c), property seized for forfeiture remains in the custody of the Attorney General, the Secretary of the Treasury, or the U.S. Postal Service. In civil judicial and criminal forfeiture cases, the USMS in the district where the property is located retains custody of the property.

3.11.c.(2). **Identification of Seized Property.** Upon receiving seized property for forfeiture, the contract investigator must immediately label the property with the corresponding CATS Identification Number provided by the AFP.

3.11.c.(3). **Use of Seized Property.** The Federal Government does not have title to property seized for forfeiture until the property is declared forfeited by a court or by a seizing agency that has administrative forfeiture authority. Any use of the seized property, except where

it is necessary to maintain the property, can raise issues of liability and create the appearance of impropriety. It is both DOJ and DCIS policy that seized property that has not been forfeited will not be used.

3.11.c.(4). **Substitute Custodial Agreements.** Occasionally, property seized by DCIS is held in the custody of another agency pending its forfeiture. Where the seized property is held by another agency, the contract investigator should obtain a signed Substitute Custodial agreement.

3.11.d. **Custody of Special Property**

3.11.d.(1). **Cash**

3.11.d.(1).(a). **Guidelines.** The security and accounting problems associated with the retention of seized cash have caused a great deal of concern with DOJ and the Congress. DOJ must annually report to Congress the amount of seized cash not on deposit in the Asset Forfeiture Fund. As a participating agency in the DOJ Forfeiture Program, DCIS is required to comply with Justice Department guidelines and regulations as noted in Criminal Resource Manual, “9-111.600 Seized Cash Management.”

3.11.d.(1).(b). **Conversion of Cash.** It is DCIS policy that all cash and negotiable (bearer) instruments will be treated as high value property and converted to a financial instrument, cashier’s check, Treasury check, money order or be deposited at a Brinks-owned facility and then handed over to the USMS. Coordination with the appropriate contract investigator and Headquarters is mandatory. According to 28 CFR §0.111(I), the USMS serves as custodian of seized and forfeited assets. All costs associated with converting cash and negotiable (bearer) instruments will be reimbursed by the AFP.

3.11.d.(1).(c). **Depositing Seized Cash for Forfeiture**

3.11.d.(1).(c).1. Except when needed as evidence, seized cash for forfeiture must be deposited within 5 days in the Seized Asset Deposit Fund (SADF) administered by the USMS pending final forfeiture or 10 days of indictment. Please note: Once a forfeiture is complete the funds from the SADF go into the Asset Forfeiture Fund (AFF).

3.11.d.(1).(c).2. Coordination with the PD or PJD is required to ensure:

3.11.d.(1).(c).2.a. forfeiture potential is established through a civil, criminal, or administrative action (e.g., seizure warrant);

3.11.d.(1).(c).2.b. a CATS number is obtained to identify the asset;

3.11.d.(1).(c).2.c. the seized currency is converted to a cashier's check with the payee the "United States Marshals Service" if not being wire transferred to the USMS;

3.11.d.(1).(c).2.d. the CATS number is included on the check prior to turning the check over to the USMS for deposit into the SADF.

3.11.d.(1).(c).3. Documentation for funds transferred to the USMS should be filed in the official case file, along with a copy of the USMS receipt for the deposit. When appropriate, photographs or digital recordings of seized cash should be taken for later use in court as evidence.

3.11.d.(1).(d). **Exceptions to Depositing Seized Cash.** If the amount of seized cash for forfeiture to be retained for evidentiary purposes is less than \$5,000, an exception to retain the cash must be granted to the AUSA by a supervisory prosecutor within the USAO. If the amount of seized cash to be retained for evidentiary purposes is \$5,000 or greater, the request for an exception must be forwarded to AFMLS. The request is to be filed by the prosecuting attorney. The AFP will be notified by the case agent and/or contract investigator that a request for exemption is being sought and a copy of the approved exemption should be forwarded to the AFP.

3.11.d.(1).(e). **No Determination Made as to Forfeiture.** In instances where a prosecuting attorney has not made a determination whether cash seized subsequent to an arrest and/or search warrant will be forfeited, the funds will be deposited in a designated DCIS HQ Bank of America (BOA) account within 5 days of seizure. Once a determination is made that cash deposited to the DCIS HQ BOA account is to be forfeited, the AFP will be contacted to coordinate a wire transfer of the funds to the USMS SADF. If a determination regarding forfeiture has not been established within 30 days, the funds are required to be returned to the appropriate party. If the funds are to be forfeited, they must be transferred to the USMS with the appropriate supporting documentation (e.g., seizure warrant) within 60 days.

3.11.d.(2). **Buy Money.** Buy money that can be identified by serial numbers or markings must be separated from money to be forfeited by DCIS. Recovered buy money must be retained and recorded by the case agent. Buy money will not be forfeited.

3.11.d.(3). **Foreign Currency.** When foreign currency is seized, the currency should be converted to a U.S. cashier's check, U.S. Treasury check, or U.S. money order, made payable to the USMS, and forwarded to the appropriate USMS office. The currency may also be wire-transferred directly to the USMS; coordination with the AFP is required.

3.11.d.(4). **Bank Accounts.** If a non-interest-bearing account is seized, the seizure warrant should specify the bank account number, as well as the exact amount to be seized, if known. In administrative forfeiture cases, the bank should provide a check, made payable to the Federal agency responsible for conducting the forfeiture. In civil judicial or criminal forfeiture cases, the bank should provide a check, made payable to the USMS for deposit into the DOJ Seized Deposit Fund.

3.11.d.(5). **USPS Money Orders**

3.11.d.(5).(a). **Seizing Agency.** Immediately following seizure, the seizing agency should send (1) the serial numbers, (2) the amount of each money order, and (3) a statement that the Government has received the money orders and is entitled to them under forfeiture laws to the following address:

National Money Order Coordinator
St. Louis Postal Data Center
P.O. Box 388
St. Louis, MO 63166-0388

The seizing agency should also provide the USMS with a copy of this letter at the time the money orders are transferred to the USMS for custody.

3.11.d.(5).(b). **USMS.** Upon forfeiture of the money orders, the USMS will (1) complete a domestic money order inquiry, PS Form 6401, for each money order; and (2) return the form, via registered mail, with the original money order to the national money order coordinator, along with the appropriate legal documentation showing that the Government is entitled to receive the proceeds.

3.11.d.(6). **Personal and Cashier's Checks**

3.11.d.(6).(a). **Seizing Agency.** Immediately following seizure, the seizing agency, in conjunction with the USAO, should:

3.11.d.(6).(a).1. obtain a restraining order or seizure warrant, under the applicable criminal or civil forfeiture statute, directing the financial institution upon which the check is drawn to either:

3.11.d.(6).(a).1.a. take necessary steps to maintain funds sufficient to cover the check, in the case of a restraining order; or

3.11.d.(6).(a).1.b. release funds in the amount of the check, in the case of a seizure warrant;

3.11.d.(6).(a).2. serve the restraining order or seizure warrant on the financial institution; and

3.11.d.(6).(a).3. provide a copy of the restraining order or seizure warrant to the USMS at the time the check is transferred for custody. In the event that a seizure warrant is obtained, the check should be voided and returned to the bank when it is no longer needed as evidence.

3.11.d.(6).(b). **USMS.** The USMS will accept custody of all checks after the investigative agency has contacted the bank on which they were drawn and negotiate the checks after receipt of a declaration or order of forfeiture in accordance with established procedures.

3.11.d.(7). **Certificates of Deposit**

3.11.d.(7).(a). **Seizing Agency.** Immediately following seizure or restraint, the seizing agency should (1) notify the bank that issued the certificate of deposit that it has been seized or restrained for forfeiture, and (2) instruct the bank officials to take whatever steps are necessary to freeze the funds covered by the certificate so the certificate of deposit will be negotiable by the USMS after forfeiture.

3.11.d.(7).(b). **USMS.** The USMS will take appropriate action, in accordance with established procedures, to liquidate the certificate of deposit after forfeiture.

3.11.d.(8). **Traveler's Checks**

3.11.d.(8).(a). **Seizing Agency.** Immediately following seizure, the seizing agency should (1) notify the company issuing the checks that they have been seized for forfeiture and (2) determine what procedures will be required in order to redeem the checks. If they can be redeemed prior to forfeiture, (1) take appropriate steps to liquidate the checks and (2) have the issuing company issue a cashier's check to the USMS. If liquidation cannot occur until after forfeiture, turn the checks over to the USMS with verification that the issuing company has been notified.

3.11.d.(8).(b). **USMS.** The USMS will accept custody of all traveler's checks that cannot be liquidated until after forfeiture. Upon receipt of a declaration of forfeiture, the USMS will liquidate the asset in accordance with established procedures.

3.11.d.(9). **Stocks and Bonds.** Immediately upon executing the seizure warrant against stocks or bonds, the issuing company that holds the stock or bond certificates should advise the case agent of the stock/bond price at the time of seizure. This will provide the appraised value for entry into the CATS system. Do not allow the brokerage firm to liquidate the stocks or bonds until after a Declaration of Forfeiture or Final Forfeiture Order is received.

3.11.d.(10). **Savings Bonds**

3.11.d.(10).(a). If DCIS seizes U.S. Savings Bonds, the contract investigator or case agent must immediately notify the Department of Treasury, by certified letter, of the seizure. The letter should include the savings bond serial number, bond denominations, to whom they are payable, and the reason they were seized.

3.11.d.(10).(b). This letter should be sent to the Bureau of Public Debt, Savings Bond Division, Parkersburg, WV 26106-0001. In judicial forfeitures, the USMS should be provided with a copy of the letter at the time the savings bonds are transferred to USMS custody.

3.11.d.(11). **Airline Tickets.** If airline tickets are seized, the contract investigator and/or case agent should immediately notify the issuing carrier of the Government's intention to forfeit the tickets. The contract investigator or case agent must determine the procedures required to redeem the tickets from the issuing carrier. If the tickets can be redeemed prior to forfeiture, take appropriate steps to liquidate the ticket and have the issuing carrier issue a cashier's check made payable to the USMS. If redemption cannot occur until after forfeiture, obtain verification from the issuing carrier that the tickets are the subject of a pending Federal forfeiture case.

3.11.d.(12). **Firearms**

3.11.d.(12).(a). All firearms and ammunition must remain in the custody of the case agent through disposal.

3.11.d.(12).(b). The contract investigator and/or the case agent should ensure that the written results from investigative inquiries are included in the case file. This includes inquiries with the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATFE) Trace Summary for each firearm. Contact your local ATFE office to determine the current procedures for requesting a firearm trace.

3.11.e. **Storage**

3.11.e.(1). **Authority.** Pursuant to 18 U.S.C. §981(c), property seized for forfeiture remains in the custody of the Attorney General, the Secretary of the Treasury, or the U.S. Postal Service. Contact the USMS to arrange for storage of all property seized for forfeiture.

3.11.e.(2). **Storage Facilities.** Additional resources for storage facilities may be obtained by contacting the Postal Inspection Service or counterparts from FBI or DEA in the district of seizure.

3.12. **Remission and Restoration**

3.12.a. **Introduction.** The DOJ-AFP requires the returning of assets to victims of financial crimes whenever possible. There are two different remedies for returning assets to victims: Petitions for Remission or Restoration. Some of these remedies are available prior to the forfeiture of the property as in Restoration. In contrast, Petition for Remission is available only after the property has been forfeited.

3.12.b. **Petition for Remission.** The Attorney General or a seizing agency may return forfeited property to an owner or lien holder of the property, or to a victim of the crime related to the underlying forfeiture, if certain eligibility criteria are met. The Federal regulations governing remission are at 28 CFR §9. This brochure addresses remission of judicial forfeitures that are handled by the Asset Forfeiture Laundering Section.

3.12.c. **Restoration.** Restoration is used when the Attorney General, at the request of a U.S. Attorney, authorizes the use of forfeited funds to pay restitution to the victim of a criminal offense. Forfeited funds may be applied to the restitution order only if no other funds are available to fulfill the defendant's restitution obligation. Restoration eliminates the victim from having to file a petition for remission.

3.12.d. **Petition Investigations**

3.12.d.(1). **Petition.** A petition investigation must be completed for each petition for remission or mitigation filed with the USAO.

3.12.d.(2). **Seizing Agency.** The investigation is conducted by the seizing agency with the results summarized in a petition report.

3.12.d.(2).(a). **Document Analysis and Verification.** The petition and supporting documents should be reviewed to determine the petitioner's interest in the property. The supporting documents should be examined for accuracy and validity. If necessary, obtain copies of title documents such as deeds, registrations, titles, or certificates from issuing agencies to verify ownership. Copies of sales document, financing agreements, and other credit documents should be obtained if the petitioner is a lien-holder. If documentation is not included with the petition, a letter should be sent to the petitioner requesting additional documentation to support the petition. If additional documentation is not received, the petition may be denied.

3.12.d.(2).(b). **Database Queries.** Use databases to verify statements contained in the petition. An NCIC check should be done in each case to determine if the property is listed as stolen. A check of Federal, state, and local criminal history databases should be conducted to determine if the violator has a criminal history that may have been known to the petitioner.

3.12.d.(3). **Interviews.** Interviews should be conducted with the petitioner and other individuals named in the petition. Interviews should also be conducted with anyone who can verify the statements made in the petition.

3.12.d.(3).(a). **Seller.** An interview should be conducted with the seller of the property to determine if the information provided by the petitioner is valid. The interview should include questions concerning the details of the purchase or acquisition of the property, particularly the form of payment and whether the purchase was made on behalf of another individual.

3.12.d.(3).(b). **Lien-holder.** If a lien-holder is involved, obtain details of their financial interest in the property. If not provided, request supporting documentation to confirm the statements made in the petition.

3.12.d.(3).(c). **Other Sources.** By interviewing other sources, such as neighbors, relatives, and co-conspirators, it is possible to determine the petitioner's knowledge of the property's illegal use by the violator or the violator's criminal record.

3.12.d.(3).(d). **Informant.** If an informant was used during the investigation, determine if the informant can verify the petitioner's knowledge of the violator's record, criminal violation, or other circumstances that would indicate an illegal use of the property.

3.12.d.(4). **Right to Financial Privacy Act.** Occasionally, a petitioning financial institution refuses to provide information regarding the loan because of the Right to Financial Privacy Act (12 U.S.C. §3401). However, Section 3403(d)(1) of the Act provides release of this information by the financial institution to the Government where it is incident to the perfection of a security interest the financial institution has in the property. Failure to provide the information may result in denial of the petition.

3.12.e. **Petition Report**

3.12.e.(1). A petition report, in the format of an Investigative Memorandum, must be completed within 45 days of the date the petition was received. The petition report summarizes the petition investigation and concludes with a recommendation to either grant or deny the petition. The petition report is transmitted with a cover letter signed by the SAC, with his or her concurrence of the petition report recommendation.

3.12.e.(2). The petition report must contain the following information:

3.12.e.(2).(a). Seizure number;

3.12.e.(2).(b). Judicial case name and number (if forfeiture is judicial);

3.12.e.(2).(c). Date and place of seizure;

3.12.e.(2).(d). Detailed narrative of seizure and basis for forfeiture;

3.12.e.(2).(e). Petitioner's name, address, and Social Security number or Federal tax identification number;

3.12.e.(2).(f). If represented by an attorney, the name and address of petitioner's attorney;

3.12.e.(2).(g). Petitioner's interest in the property;

3.12.e.(2).(h). Whether the petitioner had knowledge that the property was

or would be used in any violation of the law;

3.12.e.(2).(i). Whether the petitioner had knowledge of the particular violation that subjected the property to seizure and forfeiture;

3.12.e.(2).(j). Whether the petitioner had knowledge that the user of the property had any record for violating laws of the United States or of any state for related crime;

3.12.e.(2).(k). Whether the petitioner can show that all reasonable steps were taken, considering the information that was or should have been known to the petitioner at the time, to prevent the illegal use or acquisition of the property;

3.12.e.(2).(l). Any other petitions regarding the same property;

3.12.e.(2).(m). All relevant information, including whether the petitioner refused to cooperate or gave contradictory information; and

3.12.e.(2).(n). The recommendation of the SAC whether the petition should be granted, granted in part, denied, or denied in part.

3.12.f. **Petition Decisions – Civil Judicial and Criminal.** The case agent with assistance from the AFP will send a letter to the U.S. Attorney – Petition for Remission or Mitigation, the original petition report, and a copy of the petition to the appropriate USAO. A copy of the report and the original petition should be retained in the official seizure file. The USAO forwards the petition, DCIS and AUSA recommendations, and other relevant information to the DOJ. The Director of the Asset Forfeiture and Money Laundering Section rules on petitions in civil judicial and criminal forfeiture cases. The Director also rules on requests for reconsideration and petitions for restoration of proceeds from forfeited property when the forfeiture action is judicial.

CHAPTER 5

RIGHTS WARNINGS

<u>Contents</u>	<u>Section</u>
General	5.1.
Definitions	5.2.
Background	5.3.
Warnings Policy—Civilian Suspects in Custody	5.4.
Warnings Policy—Military Suspects	5.5.
Requirements of Article 31(b) UCMJ (Military Rules of Evidence 305) Warnings	5.6.
Situations Where Article 31(b) UCMJ Warnings Are Required	5.7.
When a Military Member Exercises or Waives His/Her Rights	5.8.
Administrative Warnings Policy	5.9.
Presence of Union and Other Third Party Representation During Investigative Interviews	5.10.
Consular Notification and Access	5.11.

5.1. General. This chapter prescribes policies and procedures on providing rights warnings in connection with interviews and interrogations conducted by special agents of the Defense Criminal Investigative Service (DCIS), Office of the Inspector General of the Department of Defense (OIG DoD). Guidance is provided regarding rights warnings in custodial and noncustodial situations, as well as warnings to persons subject to the Uniform Code of Military Justice (UCMJ). Also included is guidance regarding the use of rights warnings in administrative investigations and the rights of DoD personnel to union and third party representation during interviews.

5.2. Definitions. The following definitions apply as used in this chapter.

5.2.a. **Custody.** Custody is the placing of an individual under arrest or otherwise restricting the individual's freedom of action in any significant way (see paragraph 5.4.c. for a further explanation of what might constitute deprivation of freedom).

5.2.b. **Subject/Suspect.** This is a person whose involvement in the commission of some violation of existing law is considered a reasonable possibility.

5.2.c. **Witness.** A witness is a person, other than a subject/suspect, who possesses or is believed to possess factual information concerning the matter under investigation. A witness may be a victim, a complainant, an accuser, an eyewitness to an incident, a person having knowledge of certain facts, a record custodian, an expert laboratory technician, and so forth.

5.2.d. **Interrogation.** Any formal or informal questioning in which an incriminating response is either sought or is a reasonable consequence of such questioning, typically the questioning of a suspect, is considered an interrogation.

5.2.e. **Interview.** An interview is the questioning of an individual who either has or is believed to have factual information, not self-incriminating, which is of interest to the investigator. An interview is the questioning of a witness, as compared to an interrogation, which is used to question a subject/suspect. See DCIS Special Agents Manual (SAM) Chapter 4, “Interviews and Interrogations,” for further policy and guidance.

5.3. Background. Individuals who are interviewed or interrogated by a DCIS Special Agent may under certain circumstances have rights or obligations that will affect the interview or interrogation process. Frequently, some type of warning prior to an interrogation may be required. The Fifth and Sixth Amendments to the U.S. Constitution provide individuals with basic guarantees to be free from compulsory self-incrimination and to have the assistance of counsel for their defense. Also, Federal statutes guarantee protection to certain classes of Government personnel. For example, Title 5, United States Code (U.S.C.), section 7114(2) provides that a Government employee may request the presence of a union representative during an examination of that employee under certain conditions. Members of the Armed Forces also have *unique* rights under Article 31 of the UCMJ (10 U.S.C. 831) that may come into play earlier than *Miranda-type* rights afforded to civilians (reference SAM Chapter section 5.6 through 5.8 for additional guidance). Lastly, certain obligations and requirements can be placed on Government personnel, both civilian and military, to cooperate with investigations and to answer questions regarding their official duties. Careful application of the guidance and procedures in this chapter is necessary to ensure that individual rights are scrupulously protected and that information obtained from an interview or interrogation is admissible in subsequent legal or administrative proceedings.

5.4. Warnings Policy—Civilian Suspects in Custody

5.4.a. DCIS Special Agents are required to advise suspects that are in custody of their constitutionally protected rights and to secure an acknowledgment and waiver of those rights prior to any interrogation. The suspect must first be advised of the names and official identities of the interrogating special agents and the nature of the inquiry. The advisement and waiver requirements must be accomplished before interrogating a suspect about a crime when the suspect:

5.4.a.(1). has been deprived of freedom of action in a significant way;

5.4.a.(2). has been arrested and is in Federal custody, state custody, or the custody of a foreign government;

5.4.a.(3). whether presently in custody or not, has been previously arrested or otherwise formally charged, with prosecution pending, and the subject matter of the interrogation concerns the pending charge or a related offense unless the suspect has a lawyer present with him.

NOTE: See SAM Chapter 22, “Juveniles and Criminal Investigations,” for a discussion of juveniles.

5.4.b. DCIS Form 6 (Revised), Warning and Waiver of Rights Form (Civilian-Custodial) (Attachment A), shall be used to advise civilian suspects that are in custody of their rights and to secure a waiver prior to any custodial interrogation.

5.4.b.(1). The Fifth Amendment to the U.S. Constitution provides that no person shall be compelled in any criminal case to be a witness against himself/herself. The Sixth Amendment provides that the accused shall have the right to counsel for his/her defense in all criminal prosecutions.

5.4.b.(2). In *Miranda v. Arizona*, 384 U.S. 436 (1966), the Supreme Court ruled that when an individual is in custody or deprived of freedom in any significant way and is going to be interrogated for evidence of his/her own guilt, procedural safeguards must be employed to protect the Fifth and Sixth Amendment rights of the suspect. The required procedural safeguards consist of warning and waiver. An individual in custody must be warned of his/her right to an attorney and to remain silent, and must knowingly and intelligently waive those rights or be afforded their protections before questioning by a law enforcement officer.

5.4.c. The Supreme Court made it clear that custody and interrogation are essential conditions in applying the *Miranda* rule.

5.4.c.(1). **Custody.** Whether an individual is in custody is a crucial question (one with which law enforcement personnel frequently have difficulty) in determining whether a *Miranda* warning (DCIS Form 6) is required. One reason for the difficulty is that custody in the context of *Miranda* refers to any significant deprivation of an individual’s freedom of action. In *United States v. Mendenhall*, 446 U.S. 544 (1980), the Court held that in determining whether a suspect was in custody at a particular time, the only relevant inquiry is how a reasonable person in the suspect’s position would have understood the situation. Determining when a suspect has been deprived of his/her freedom of action in any significant way and is in custody depends on a variety of circumstances. The following factors are the ones most commonly used by the courts to determine whether custody exists.

(b)(7)(E)

(b)(7)(E)

5.5. Warnings Policy—Military Suspects. Under Article 31, UCMJ, investigators are obligated to administer a rights warning as soon as the investigator suspects that an individual that is subject to the UCMJ has committed a crime. It is the policy of DCIS to advise military suspects of their rights under the UCMJ in the same manner as if a criminal investigator that is subject to the UCMJ was conducting the interrogations, unless otherwise directed by the Department of Justice attorney responsible for the investigation in accordance with DoD Instruction 5525.07. According to DoDI 5525.07, “...when DoD procedures concerning apprehension, search and seizure, interrogation, eyewitnesses, or identification differ from those of DoJ, DoD procedures will be used, unless the DoJ prosecutor has directed that DoJ procedures be used instead. DoD criminal investigators should bring to the attention of the DoJ prosecutor, as appropriate, situations when use of DoJ procedures might impede or preclude prosecution under Reference (f).”

5.6. Requirements of Article 31(b) UCMJ (Military Rules of Evidence 305) Warnings

5.6.a. Special agents shall not interrogate or request any statement from an accused military member or a military member suspected of an offense—WHETHER IN CUSTODY OR NOT—without first advising the suspect:

5.6.a.(1). the nature of the offense under investigation;

5.6.a.(2). that he/she is suspected of having committed that offense;

5.6.a.(3). that he/she has the right to remain silent;

5.6.a.(4). that any statement made may be used as evidence against the suspect in a trial by court-martial or other judicial proceedings;

5.6.a.(5). that he/she has the right to consult with a lawyer or to have a lawyer present during the interrogation. If the suspect so desires, he/she can have a military lawyer appointed to represent him/her at the interrogation at no expense to the individual or may obtain a civilian lawyer at no expense to the Government in addition to or instead of free military counsel; and

5.6.a.(6). that he/she has the right to terminate the interrogation at any time for any reason.

5.6.b. DCIS Form 71 (Revised), Military Suspect's Warning and Waiver of Rights Form (Attachment B) shall be used to provide the advisement discussed above. The suspect shall be requested to initial each line of this advisement on the lines provided.

5.6.c. The fact that a military suspect may have known his/her rights is of no importance if warnings were required but not given. Spontaneous or volunteered statements do not require Article 31(b) warnings and are handled in the same manner as described in paragraph 5.4.c.(2).(a).

5.6.d. When Article 31(b) warnings are required and a special agent intends to question a suspect of an offense and **knows or reasonably should know** that a lawyer either has been appointed for or retained by the suspect with respect to that offense, **THE LAWYER MUST BE NOTIFIED OF THE INTENDED INTERROGATION AND THE SPECIAL AGENT SHALL NOT PROCEED WITH THE INTERROGATION WITHOUT THE CONCURRENCE OF THAT LAWYER.** In such cases, all contacts with the suspect must be through the lawyer.

5.6.e. The Court of Military Appeals has held that a statement obtained in violation of Article 31(b) is involuntary. An involuntary statement or any evidence derived therefrom may not be received in evidence against an accused military member if the accused makes a timely motion to suppress the evidence or raises an objection to it.

5.7. Situations Where Article 31(b) UCMJ Warnings Are Required

5.7.a. Article 31(b) UCMJ warnings are required in the following situations:

5.7.a.(1). investigations of military subjects with a reasonable anticipation that the subjects may be tried by courts-martial;

5.7.a.(2). joint investigations with a Military Criminal Investigative Organization where the cooperative efforts demonstrate that the two investigations (if initiated as such) have merged into an indivisible entity; e.g., investigations conducted in accordance with DoD Instruction 5505.2, "Criminal Investigations of Fraud Offenses," February 6, 2003;

5.7.a.(3). investigations in furtherance of a military investigation, e.g., an investigation to supplement an ongoing or completed military investigation; and

5.7.a.(4). investigations of crimes committed by persons subject to the UCMJ, whether committed on or outside a military installation, which are normally tried by courts-martial (see DoD Instruction 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," June 18, 2007).

5.7.b. DCIS Form 71 (Attachment B) shall be used when advising a military suspect of his/her Article 31(b) rights and obtaining a waiver of those rights.

5.8. When a Military Member Exercises or Waives His/Her Rights

5.8.a. If a military suspect chooses to exercise the privilege against self-incrimination or requests counsel under Article 31(b), questioning must cease immediately.

5.8.b. After receiving applicable warning, a military suspect may waive the rights and make a statement. The waiver must be made VOLUNTARILY, KNOWINGLY, and INTELLIGENTLY. A written waiver shall be sought on DCIS Form 71 (Attachment B). The suspect must acknowledge affirmatively that he/she understands the rights involved, affirmatively declines the right to counsel, and affirmatively consents to make a statement. The following three waiver statements should be asked:

5.8.b.(1). Do you understand your rights?

5.8.b.(2). Do you want a lawyer?

5.8.b.(3). Are you willing to make a statement?

5.9. Administrative Warnings Policy

5.9.a. Generally, one of two situations may arise during a job-related misconduct investigation. First, an employee may be given the opportunity to respond to questions regarding job-related misconduct; second, the cooperation of the employee may be considered essential enough that management requires the employee to answer questions or face dismissal for refusing to do so.

(b)(7)(E)

(b)(7)(E)

5.10. Presence of Union and Other Third Party Representation During Investigative Interviews

5.10.a. It is the policy of DCIS that representatives of employee unions shall be allowed to be present during interviews or interrogations conducted by DCIS Special Agents if requested by the person being interviewed. This policy applies to criminal and administrative investigations.

5.10.b. In *NASA v. FLRA*, 527 U.S. 229 (1999), an inspector with the Office of the Inspector General, National Aeronautics and Space Administration (NASA), interviewed a NASA employee who requested and was granted union representation. At this interview, the NASA investigator advised that the union representative was not to interrupt the question-and-answer process. The interview resulted in a complaint by the union representative that the investigator had improperly limited the union representative's participation in the interview. The union filed an unfair labor practice charge with the Federal Labor Relations Authority. The administrative law judge ruled in favor of the union, and the Court of Appeals affirmed that decision. NASA appealed to the U.S. Supreme Court, which held that Federal employees have the right to union representation during Inspector General investigations because Inspectors General are acting as representatives of agency management. This case stands for the proposition that union representatives cannot be prevented from participation in the interview, but they can be excluded if they interfere excessively with the interview process. The following

will serve as additional guidance for DCIS Special Agents regarding the union representative's participation during the interview and recommendations as to how to proceed if the union representative interferes with the interview.

5.10.b.(1). Telling a union representative to remain silent or refusing to allow comments or questions concerning possible infringement of an employee's rights has been held to be unfair labor practices.

5.10.b.(2). The union representative may take an active role in the interview by posing questions and attempting to clarify issues.

5.10.b.(3). The union representative is present to assist the employee and should be allowed to confer with the employee regarding the employee's rights.

5.10.b.(4). The union representative may not interfere with the interview, dictate answers, or take charge of the proceedings.

5.10.b.(5). The union representative may not make repeated objections or arguments for the purpose of interfering with the investigator's ability to complete the interview.

5.10.b.(6). The union representative may not coach the witness in providing answers. Answers should come from the witness.

5.10.b.(7). The investigator has the right to hear the employee's account of the matter under investigation.

5.10.b.(8). The union representative may be told that he/she may not tape-record the interview if taping is contrary to agency policy.

5.10.b.(9). The union representative has the right to consult with the employee but not necessarily outside the interview room.

5.10.b.(10). A union representative that seeks to control or disrupt the interview can be dismissed from the interview.

5.10.b.(11). If a union representative is dismissed, the employee should be offered a choice to continue the interview with a union representative or to discontinue the interview.

5.10.b.(12). If the employee still requests a union representative, an effort should be made to locate an alternative union representative.

5.10.c. Other occasions may occur when the presence of one of the following persons is needed during an interview.

5.10.c.(1). **Parents.** Normally, parents or their designated representative should be present during the interview of their minor children and should provide their consent in writing for the interview to be conducted. (See SAM Chapters 4 and 22 for further guidance.)

5.10.c.(2). **Interpreters.** Interpreters may be present during interviews where the subject has a better grasp of the matter in his/her native language. (See SAM Chapter 4 for further guidance.)

5.10.c.(3). **Others.** Certain circumstances may at times dictate allowing other individuals to be present during an interview (e.g., doctor, nurse).

5.10.d. The presence of another person will be for a specific reason germane to the interview. Observers will not act in an advisory capacity during the interview.

5.11. Consular Notification and Access

5.11.a. Summary of Requirements Pertaining to Foreign Nationals

5.11.a.(1). When foreign nationals are arrested or detained, they must be advised of the right to have their consular officials notified.

5.11.a.(2). In some cases, the nearest consular officials *must* be notified of the arrest or detention of a foreign national, regardless of the national's wishes.

5.11.a.(3). Consular officials are entitled to access to their nationals in detention, and are entitled to provide consular assistance.

5.11.a.(4). When a government official becomes aware of the death of a foreign national, consular officials must be notified.

5.11.a.(5). When a guardianship or trusteeship is being considered with respect to a foreign national who is a minor or incompetent, consular officials must be notified.

5.11.a.(6). When a foreign ship or aircraft wrecks or crashes, consular officials must be notified.

(b)(7)(E)

CHAPTER 6

STATEMENTS

<u>Contents</u>	<u>Section</u>
General	6.1.
Obtaining Signed Sworn Statements	6.2.
Obtaining Oral Statements	6.3.
Reducing Information to Writing	6.4.
Types and Format of Written Statements	6.5.
Reporting Interviews on a DCIS Form 1	6.6.
Modification of DCIS Statement Forms	6.7.
Review of Statement	6.8.
Administration of an Oath	6.9.
Security Classification of Statements	6.10.
Request for a Copy of Statement	6.11.
Acceptance of Volunteered Statements	6.12.

6.1. General

6.1.a. This chapter presents the policy and procedures for taking statements and administering oaths. These procedures apply to all Defense Criminal Investigative Service (DCIS) special agents.

6.1.b. A written statement is an official record of information provided by an individual concerning the matter under investigation of which the individual has personal knowledge. Written statements can be used to document confessions and admissions by suspects/subjects, as well as information provided by victims, complainants, and witnesses. When taken, all statements will be sworn or affirmed unless waived by the interviewee. For the purposes of this chapter, written statements will be considered the same as sworn statements and the term used interchangeably throughout. Obtaining an unsworn written statement is appropriate if the interviewee declines to take an oath or affirmation.

6.1.c. As soon as possible after the interview or interrogation, transfer (reduce) the oral statements of witnesses, victims, or suspects/subjects to written form and document on a DCIS Form 1 or as a written statement.

6.1.d. Oral statements that have been reduced to a written statement may be signed by the interviewee. When appropriate, special agents may summarize an oral statement depending on the following.

6.1.d.(1). advice of the prosecuting attorney (Assistant U.S. Attorney (AUSA), state attorney, etc.);

6.1.d.(2). importance of the information; and

6.1.d.(3). willingness of the interviewed or interrogated individual.

(b)(7)(E)

(b)(7)(E)

6.9. Administration of an Oath

6.9.a. All DCIS special agents are authorized to administer oaths in connection with official investigations. This authority is contained under section 303b, title 5, United States Code. There is no legal requirement that the written statement be taken under oath would be admissible into evidence at a trial. The governing factors for admissibility are that the statement be voluntary and be preceded by a rights warning (if appropriate).

6.9.b. Administer the oath after the individual has read the statement, made corrections if needed, and the special agent has determined that the individual is capable of reading the statement. At the time the oath is administered, the person making the statement and the person administering the oath must be in the presence of each other. All those present should stand when the person is being sworn. There is no required procedure that must be used in administering an oath. Any procedure is sufficient that appeals to the conscience of the person to whom the oath is administered, and that binds the individual to speak the truth.

6.9.c. The normal procedure for administering the oath or affirmation consists of raising the right hand by both the individual administering the oath and the individual taking the oath during the recitation of the oath and the response. Individuals who recognize special forms or rites may be sworn in their own manner or according to the ceremonies of the religion they follow. The following form of oath will normally be used.

“Do you swear (or affirm) that the statement given by you is the truth,
the whole truth, and nothing but the truth?”

An affirmative response validates the oath.

6.10. Security Classification of Statements. Statements containing classified information will contain the appropriate markings and downgrading instructions. Each portion of an unclassified document that requires dissemination control shall be portion marked, for example, (U/FOUO/LES), to show that it contains information requiring protection. DoD Manual 5200.01, Volume 2, “DoD Information Security Program: Marking of Classified Information,” February 24, 2012 (incorporating change 1, March 21, 2012), contains guidance regarding the classification of documents.

6.11. Request for a Copy of Statement. **Provide a copy of the statement** if the individual making a written statement asks for a copy. State that a copy was provided to the interviewee on the DCIS Form 1 or other investigative document. Provide a copy of the written statement to the individual’s counsel if requested. Under no circumstances will a copy of the written statement of a witness, signed or unsigned, be given to a suspect/subject or the suspect/subject’s counsel without prior approval of the prosecuting attorney.

6.12. Acceptance of Volunteered Statements. Volunteered information that is of investigative interest to DCIS or other agencies will be accepted and incorporated into a written statement. Attach this information to the DCIS Form 1. No commitment will be made to individuals that volunteer the information with regard to the disposition of the information or its effect upon any case, except that it will be forwarded to an appropriate action official. Use caution throughout the interview process to prevent the disclosure of information or to confirm the commencement or the existence of an investigation.

ATTACHMENT C

DEFENSE CRIMINAL INVESTIGATIVE SERVICE VOLUNTARY STATEMENT	
SECTION I - GENERAL	
1. Place	
2. Date/Time	
3. Names	
<p>I, _____, do hereby make the following voluntary statement to</p> <p>Special Agent, _____, who has identified himself/herself to me as a</p> <p>Special Agent of the Defense Criminal Investigative Service. I make this statement without any threats having been</p> <p>made against me or any promises extended to me.</p>	
SECTION II - STATEMENT	

DCIS FORM 3, 9-22-14 DRAFT

ADOBE LIVECYCLE DESIGNER ES

PAGE 1 of 1 PAGES

DEFENSE CRIMINAL INVESTIGATIVE SERVICE
VOLUNTARY STATEMENT CONTINUATION

SECTION I - STATEMENT CONTINUATION

SECTION II - SIGNATURES

I further state that I have read this entire statement, consisting of _____ pages, initialed all pages and corrections, and signed this statement, and that it is correct and true as written.

1. SIGNATURE	2. DATE/TIME
--------------	--------------

Subscribed and sworn to before me at _____
this _____ day of _____.

3. SPECIAL AGENT SIGNATURE (DCIS)

4. WITNESS NAME (1)

5. WITNESS SIGNATURE (1)	6. DATE
--------------------------	---------

7. WITNESS NAME (2)

8. WITNESS SIGNATURE (2)	9. DATE
--------------------------	---------

CHAPTER 10

EMERGENCY AND EXTRAORDINARY FUNDS

<u>Contents</u>	<u>Section</u>
Authority and Purpose	10.1.
General Policy	10.2.
Prohibition on Use	10.3.
Authorized Expense Categories	10.4.
UCO Budget Line Items/Terms	10.5.
Accountability	10.6.
Terms, Roles, and Responsibilities	10.7.
Preparation of Claims and Monthly Reports	10.8.
Fund Administration	10.9.
Inspection and Audit	10.10.
Correction/Collection Procedures	10.11.

10.1. Authority and Purpose

10.1.a. Title 10, United States Code (U.S.C.), Section 127, “Emergency and Extraordinary (E&E) Expenses,” (Attachment A), provides statutory authority to the Department of Defense (DoD), Inspector General for the expenditure of funds relative to “...any emergency or extraordinary expense which cannot be anticipated or classified.” The statute also provides that “...the funds may be spent on approval or authority of the...Inspector General for any purpose he determines to be proper, and such a determination is final and conclusive upon the accounting officers of the United States.”

10.1.b. Title 10, U.S.C., § 127 further provides that “the authority conferred by this section may be delegated...by the Inspector General to any person in the Office of the Inspector General, Department of Defense, (OIG DoD)...with or without the authority to make successive re-delegations.” The Inspector General, DoD has delegated approval authority of E&E to the Deputy Inspector General for Investigations (DIG INV) (Attachment B), who has delegated approval authority to the Special Agent in Charge, Investigative Operations (SAC, INV); and the Special Agents in Charge, Field Offices (SAC, FO), for the expenditure of E&E funds in accordance with the memorandum delegating authority to approve E&E expenditures (Attachment C). Approving officials may approve E&E expenditures up to only \$5,000. Expenditures exceeding \$5,000 require approval from SAC, INV. All expenditures exceeding the \$10,000 limit must be approved by DIG INV.

10.1.c. The DoD Financial Management Regulation (FMR), DoD Instruction 7000.14, is a single DoD-wide financial management regulation (Attachment D) that must be used by all DoD Components for accounting, budgeting, finance, and financial management education and training. The DoD FMR sets forth certain policies and procedures that are applicable to the management and oversight of E&E funds.

10.1.d. Defense Criminal Investigative Service (DCIS) was granted an exception by the DoD Comptroller to establish and maintain accounts at Headquarters (HQ) and six field offices. The accounts are designated for E&E and should be maintained in an interest-bearing account at each location for the purpose of administering E&E funds (Attachment E).

10.1.e. The purpose of this chapter is to proscribe the policies and procedures by which E&E funds shall be used and managed within DCIS.

10.2. General Policy

(b)(7)(E)

10.3. Prohibition on Use

10.3.a. It is OIG DoD policy not to approve expenditures for items of a personal nature, expenditures that tend to circumvent other specific provisions of law, or expenditures for entertainment of Federal officials, except when operationally necessary (e.g., when such officials are targets of a criminal investigation and the expense is incurred in furtherance of the investigation). DIG INV is held personally financially accountable for these funds and will disallow improper expenditures when monthly reports are audited at the HQ level.

10.3.b. Notwithstanding operational considerations, such as in the case of Undercover Operations (UCOs), cameo appearances, and the backstopping of Undercover Agents (UCAs), the below-listed expenditures are generally prohibited for payment with E&E funds.

10.3.b.(1). Title 5, U.S.C. § 5536 bans the use of E&E funds to supplement the pay, allowances, and entitlements of personnel employed in either a civilian or military capacity by DoD for the performance of functions within their established scope of duty.

10.3.b.(2). Title 31, U.S.C. § 1301 prohibits gifts to any employee of the U.S. Government.

10.3.b.(3). E&E funds may not be used to purchase printed stationery, to include seasonal/greeting cards, thank-you cards, etc., as these items are generally considered to be personal in nature.

10.3.b.(4). E&E funds may not be used for the entertainment of U.S. or foreign law enforcement officials for representational purposes. DoD Directive 7250.13, “Official Representation Funds,” restricts the use of such funds to “...host official receptions, dinners, and similar events, and to otherwise extend official courtesies to guests of the United States and the Department of Defense for the purpose of maintaining the standing and prestige of the United States and the Department of Defense.” Routine liaison activities do not constitute an activity that maintains the “standing and prestige” of the United States and/or DoD.

10.3.b.(5). Do not use E&E funds for normal housekeeping items of the field office or resident agency that should be procured through regular supply channels, including repairs, maintenance, and renovation projects as other procurement channels exist for such items.

10.3.b.(6). E&E funds are not to be used for the purchase of birth, death, or marriage certificates as such items are generally considered to be personal in nature.

10.3.b.(7). Do not use E&E funds for payment for transportation of investigative aids as other funding mechanisms exist for such items.

10.4. Authorized Expense Categories. E&E Expense items, not related to or covered by a Group I or Group II UCO budget item, but permissible in accordance with this chapter and in the furtherance of an authorized investigation must be categorized as an E&E Expense. All claims for expenses incurred shall be itemized on DCIS Form 75, Claim for E&E Expenses (Attachment F). The expense categories are listed below.

(b)(7)(E)

10.5. UCO Budget Line Items/Terms. All E&E expenses associated with a Group I or Group II UCO must be authorized in accordance with the provisions of SAM Chapter 9, “Undercover Operations.” E&E funding for Group I and Group II UCOs is authorized on the basis of individual line items as well as an overall budget amount for a specified 6-month period. Therefore, funding cannot be increased or moved from one line item to another without the prior approval of the appropriate DCIS UCO ***authorizing*** official, who may be different than the E&E ***approving*** official. All UCO E&E expenditures must be categorized into one of the following budget line items.

(b)(7)(E)

(b)(7)(E)

10.6. Accountability

10.6.a The UCO **authorizing** official for all Group I UCOs is the DIG INV. Therefore, any increase in overall funding amounts on Group I UCOs must be approved by the DIG INV. The **authorizing** official for all Group II UCOs is the SAC, FOs. Therefore, any increase in overall funding amounts on Group II UCOs (subject to the limitations for Group II funding as specified in SAM Chapter 9, “Undercover Operations”) must be approved by the SAC, FO. Any increase in overall funding amounts on Group II UCOs **must** be coordinated with the PD, SO, **prior** to SAC, FO approval in order to ensure that sufficient funds are available.

10.6.b. Frequently, funds need to be reprogrammed from one UCO budget line item to another for successful mission accomplishment. In order to reduce the administrative burden associated with the submission of routine reprogramming requests from the SAC, FOs, through the Investigative Operations Directorate to the DIG INV, SAC, FOs may approve the reprogramming of funds for Group I UCOs. When funds have been reprogrammed relative to a Group I UCO, an e-mail will be submitted from or through the SAC, FO to the PD, SO, providing the details of the reprogramming request. The PD, SO will review the details and if the reprogramming appears to be inconsistent with the approved UCO, the request will be coordinated with the SAC, INV. Concurrence by the SAC, INV will be assumed absent any notification within 21 calendar days of the initial request. Documentation of all reprogramming requests and approvals must be filed in the official case file for future reference.

10.6.c. All DCIS personnel are required to properly use and account for E&E funds in accordance with this chapter. ***Regardless of the dollar amount, all claims must be supported by documentation, such as original receipts and/or memoranda for the record (MFR).*** Copies of receipts or MFRs should be attached to the DCIS Form 75. All original receipts and MFRs shall be maintained at the originating office and copies also will be maintained by the E&E custodian. Due to the covert nature of such funds and the fact that, by statute, the expenditure of such funds is not subject to the same level of scrutiny as other public funds, accountability must be maintained in a more stringent fashion than with other appropriations of

the Federal government. It becomes necessary, therefore, to avoid any and all expenditures that are or may appear to be improper. Personnel expending E&E funds must always consider the value of the item or information being obtained as well as the overall propriety and legality of the expenditure before making the expenditure. Personnel authorized to expend E&E funds are responsible for familiarizing themselves with and following the procedures established in this chapter. Questionable expenditures will be referred to the appropriate approving official (as described below), or his/her suitably designated appointee, for clarification. Additional guidance may be sought from the PD, SO, and/or a legal advisor in OGC. However, only the opinions provided by an OGC legal adviser will afford protection for officials relative to the administration of E&E funds.

10.6.d. Military and civilian Government personnel not attached to DCIS but under DCIS supervision may be provided E&E funds for specific and immediate use. As these personnel will usually not be aware of the contents of this chapter, including the prohibitions of use provisions, the supervising DCIS employee shall be responsible for proper safeguarding and utilization of E&E funds. Accordingly, liability for the funds shall remain with the DCIS employee and the DCIS employee will prepare all claims associated with the expenditure of such funds. The claims will include the name(s) of non-DCIS personnel involved in the expenditure of E&E funds.

10.6.e. Expenditures of E&E funds will be reviewed by the appropriate chain of command to ensure compliance with this chapter. Deficiencies and/or discrepancies will be corrected or fully explained when identified. Additionally, all E&E claims will be reviewed by DCIS HQ E&E fund custodian for completeness, accuracy, and compliance with this chapter. Furthermore, all claims will be reviewed by the OIG Comptroller for completeness and accuracy. Deficient claims will be referred to the submitting office for correction or explanation. Such referrals will be tracked until resolved. Unresolved discrepancies will be referred to the DIG INV for appropriate resolution.

10.6.f. Any indication of a *willful failure* to follow the provisions of this chapter, particularly when a loss of accountability has occurred, will result in a prompt referral to the SAC, INV for investigation and appropriate action.

10.7. Terms, Roles, and Responsibilities

10.7.a. The below-listed terms are used in the administration of E&E funds.

10.7.a.(1). **Advances Pending.** Describes E&E funds that have been provided to a DCIS employee by an E&E custodian in advance of an anticipated expenditure. These advances do not constitute transfers out of an E&E fund account as they are pending advances until the funds are expended or returned to the E&E fund custodian. These advances are maintained in the possession of the agent receiving the funds as pending rather than as “cash-on-hand.”

10.7.a.(2). **Approving Official.** The person authorized to approve an expenditure of E&E funds. Approving officials include each SAC, FO; SAC, INV; and the DIG INV. The Assistant Special Agents in Charge (ASACs) and PD, SO, may serve as approving officials if authority has been formally delegated in writing. Approving officials may only approve General or UCO expenditures of E&E funds up to \$5,000. Expenditures exceeding \$5,000 require approval from the SAC, INV. The DIG INV is responsible for providing advance approval for UCO and general expenditures exceeding \$10,000. SAC, FO or a delegated approving official should forward the request via e-mail to SAC, INV for review and routing. Approving officials are considered “departmental accountable officials” within the provisions of 10 U.S.C. § 2773a and DoD Instruction 7000.14 and as such, must properly execute DD Form 577, Appointment/ Termination Record – Authorized Signature, prior to approving the expenditure of E&E funds.

10.7.a.(3). **Authorizing Official.** The person authorized to approve the initiation of a UCO. Group I UCOs may be authorized only by the DIG INV. Group II UCOs may be authorized only by the SAC, FOs, with legal concurrence from OGC.

10.7.a.(4). **Cash-on-Hand.** Describes E&E funds that are maintained in the form of cash by the appointed E&E fund custodian.

10.7.a.(5). **Commander.** Formally referred to as the “Convening Authority,” describes the senior management official with authority to appoint an Investigating Officer relative to the investigation of a fiscal irregularity as more fully described in Volume 5, Chapter 6, of the DoD FMR (Attachment M). The SAC, INV, shall act as the Commander relative to loss investigations involving personnel within their chain of command. In situations where an approving official (who would be the Commander) is responsible for the irregularity, or where personnel in different field offices are involved, the DIG INV will act as the Commander.

10.7.a.(6). **Expenditure.** Describes the actual payout of funds. For example, when funds are paid to a vendor in exchange for goods and/or services, an E&E expenditure has occurred. However, when funds have been obligated, but not actually expended (e.g., a charge to a credit card account), an E&E fund expenditure has not occurred. Funds advanced to an agent in anticipation of a future expenditure are not considered *expended* until the funds have actually been paid to a third party and receipts for such expenditures have been provided to the E&E fund custodian. The only exception to this requirement is the expenditure of funds in connection with TDY travel where certain costs (e.g., the payment of covert credit card expenses) have been incurred, but not yet paid.

10.7.a.(7). **Expense Category.** Describes the appropriate E&E expense category as more fully described in section 10.4. above. Only one of the specified categories should be used to describe the nature of the expense. If the expense relates to an undercover operation, the expense should be categorized as “Undercover Operation” and further classified in accordance with the appropriate UCO budget line item, as more fully described in section 10.5. above.

10.7.a.(8). **Fiscal Irregularity.** Defined as a situation where there has been either (1) a physical loss of cash, vouchers, negotiable instruments, or supporting documents; or (2) an erroneous payment.

10.7.a.(9). **Funds Available.** Describes the total funds available in a general E&E or undercover fund account at any given point in time. The funds available shall include cash-on-hand, bank account balances, and pending cash advances.

10.7.a.(10). **Investigating Officer.** Describes the individual that is appointed by the Commander to investigate alleged fiscal irregularities.

10.7.a.(11). **Loss of Accountability.** Defined as a situation where an E&E fund account cannot be reconciled and the disposition of funds cannot be determined based on available supporting documentation.

10.7.a.(12). **Revolving Advance.** Describes amounts that are continually advanced to DCIS field offices in support of E&E fund accounts.

10.7.a.(13). **Transfer.** Describes funds transferred between E&E accounts. For example, when funds are moved from the HQ general E&E fund account to a field office general E&E fund account, the funds have been transferred out of one account and into another. Funds “advanced” to an agent to be expended relative to the affected E&E account are not considered to have been “transferred” out of the account and such funds should continue to be reported as “funds available” and also included as a “pending advance ” on DCIS Form 75A, Monthly Summary Report (Attachment N).

10.7.a.(14). **Undercover Budget Line Item.** Describes the approved UCO budget line item as more fully explained in section 10.4. above.

10.7.b. The roles and responsibilities concerning the management and administration of E&E funds are described below.

10.7.b.(1). **DIG INV.** Only the DIG INV is responsible for providing advance approval for UCO expenditures of E&E funds in excess of \$10,000. If several related expenditures are expected to exceed \$10,000 (e.g., two payments of \$8,000 each for the purchase of stolen property), prior approval by the DIG INV is required. The SAC, INV is responsible for providing advance approval of general or UCO E&E funds up to \$10,000 and the SAC, FOs are responsible for providing advance approval of general or UCO E&E funds up to \$5,000. Prior approval should be requested via e-mail in order to expedite the transfer of E&E funds.

10.7.b.(2). **Assistant Inspector General, Investigative Operations (AIGI-INV).** The AIGI-INV may be called upon to serve as the Commander relative to the investigation of a fiscal irregularity. The AIGI-INV is responsible for providing advance approval for general expenditures exceeding \$10,000.

10.7.b.(3). **SAC, FOs and the SAC, INV.** SAC, FOs and the SAC, INV are responsible for providing advance approval for all expenditures of E&E funds in accordance with the delegation memorandum. Requests for funds should be sent via e-mail in order to expedite the transfer of funds to the E&E Account. SAC, FO, and the SAC, INV may delegate this authority in writing to the ASACs, and copies must be provided to the PD, SO. The SAC, FOs, and the SAC, INV, are also responsible for appointing primary and alternate E&E fund custodians in writing, a copy of which must be provided to the PD, SO. Additionally, the SAC FOs and SAC, INV, or the ASAC, or his/her designee, must conduct surprise audits of all E&E fund accounts within their area of responsibility in accordance with the requirements set out in section 10.10. below. The SAC, FOs, and SAC, INV, may be required to serve as the Commander relative to the investigation of alleged fiscal irregularities. The SAC, INV, is further responsible for appointing in writing an HQ certifying officer as more fully described in paragraph 10.7.b.(8). below.

10.7.b.(4). **PD, SO.** The PD, SO is the primary point of contact within the Investigative Operations Directorate for addressing questions and coordinating E&E funding issues. The PD, SO is further responsible for maintaining general visibility of E&E funds available balances and total expenditures to date to ensure that (1) operational requirements can be met; (2) spending is consistent with established budgetary constraints; and (3) upper management is kept apprised of significant E&E funding concerns. In the event that a request for E&E funds cannot be met from the HQ E&E account, the PD, SO, will identify funds available in one or more field accounts and will direct the custodian(s) of that (those) E&E accounts to transfer funds to the requesting E&E account. The PD, SO will maintain a central file identifying all DCIS personnel who are currently appointed as E&E fund custodians, as well as those personnel to whom approval authority has been delegated.

10.7.b.(5). **HQ E&E Fund Custodian.** The HQ E&E Fund Custodian is responsible for administering the HQ E&E fund account. The HQ E&E fund custodian requests fund replenishments and disburses funds to other E&E accounts as directed by the PD, SO. The HQ E&E fund custodian must maintain visibility of all funds available balances in order to ensure that DCIS does not exceed its cash holding authority. The HQ E&E fund custodian assists the PD, SO in maintaining general visibility of E&E funds available balances and expenditures to date and ensures that the PD, SO is aware of significant E&E issues. The HQ E&E fund custodian prepares the monthly E&E expense report and provides it directly for audit to the OIG Comptroller. After audit by the OIG Comptroller, the HQ E&E fund custodian will prepare DoD Form 281, Voucher for Emergency or Extraordinary Expense Expenditures, for signature by the AIGI-INV and the OIG Comptroller.

10.7.b.(6). **SAC Internal Operations (SAC, INT).** SAC, INT receives from the HQ E&E fund custodian the quarterly E&E expenditures, which are reviewed for completeness and accuracy. The SAC, INT further provides input as required to the OIG Comptroller.

10.7.b.(7). **UCO Program Manager (UCO, PM).** The UCO, PM is responsible for tracking UCO expenses against approved budgets, including enhancements and

reprogramming of funds between budget line items. The UCO, PM will receive the requests for funding and if the request is in line with the approved budget and will not cause the UCO to exceed its budget authorization, the UCO, PM will coordinate the request with the HQ E&E fund custodian for funding.

10.7.b.(8). **SAC, INV.** The SAC, INV is responsible for reviewing all monthly E&E expense reports for the purpose of verifying that all expenses were appropriate (based on the supporting documentation provided), properly documented, and made in accordance with established policy. The SAC, INV will certifying the monthly reports, which the HQ E&E fund custodian will then provide to the OIG Comptroller for auditing and filing by the HQ records administrator.

10.7.b.(9). **E&E Fund Custodians.** E&E fund custodians are DCIS personnel who are responsible for maintaining an E&E fund account for which they have been designated as the custodian, including UCO E&E accounts. Custodians must be appointed in writing by the appropriate approving official. E&E fund custodians are responsible for receipt and disbursement of funds; transferring funds to other E&E fund custodians; maintaining appropriate bank accounts and cash balances; tracking any and all advances made to DCIS personnel and third parties; and reconciling the E&E fund account as required by section 10.9. below.

10.7.b.(10). **First-Line Supervisors.** First-line supervisors are supervisory personnel responsible for reviewing and signing each claim form prior to submission to the appropriate approving official. The signature of the first-line supervisor indicates that he/she has reviewed the claim and determined that the claimed expenses have been properly documented, were incurred in connection with official business, and are proper for payment in accordance with this chapter.

10.7.b.(11). **Claimants.** Claimants are DCIS personnel who personally expend E&E funds. Non-DCIS personnel cannot be E&E claimants. Claimants are responsible for obtaining prior approval of anticipated E&E expenses and properly documenting each expense in accordance with section 10.8. below.

10.7.b.(12). **OIG Comptroller.** The OIG Comptroller is responsible for verifying the completeness and accuracy of all DCIS E&E monthly reports and certifying the DoD Form 281. The OIG Comptroller is also responsible for at least one annual site visit.

10.8. Preparation of Claims and Monthly Reports

10.8.a. Claimants must prepare a DCIS Form 75 for any expenditure of E&E funds. Claimants may also be required to prepare a claim form for expenses incurred by third-parties where operational circumstances dictate (e.g., where a UCA from another agency purchases evidence using DCIS E&E funds provided by the claimant). If expenses are claimed for expenditures made by a third party, the claim form or supporting documentation should fully identify the third party who expended the funds.

10.8.b. Claimants should list expenses on the DCIS Form 75 only for expenditures such as cash, checks, or recurring expenses. The only exception to this requirement is when the claim is for reimbursement of travel expenses (see paragraph 10.4.h. above for more information).

10.8.c. Every effort should be made to avoid incurring unnecessary late fees and finance charges. In the event that late fees and finance charges are incurred as the result of legitimate operational circumstances, justification for paying the expense with public funds *must* be included with the claim. Failure to plan ahead or regularly check a covert mailbox is not a legitimate operational circumstance.

10.8.d. All claims must be supported by documentation, such as copies of receipts and/or MFRs that document the expenditure. Redacted copies of receipts must be provided when the original receipt may compromise an alias persona or identify a documented source. In the event a receipt for expenditure is not available, an MFR will be submitted with the claim documenting the expense and explaining the reason why a receipt could not be provided. Credit card statements are acceptable supporting documentation for certain recurring expenses. If a finance charge or late fee is claimed, justification for the expense must be provided. Under no circumstances should a credit card account be permitted to become delinquent. In the event that an original receipt is smaller than 8½ by 11 inches, it should be taped to a blank 8½ by 11 inch sheet of paper to prevent loss of the receipt and facilitate photocopying. **DO NOT INCLUDE ORIGINAL RECEIPTS OR ACCOUNT STATEMENTS CONTAINING SOURCE-IDENTIFYING OR UCA ALIAS IDENTIFICATION.** This is necessary to protect the identity of sources and to prevent the potential compromise of sensitive information relative to UCAs.

10.8.e. Monthly expense reports shall be prepared and submitted to the HQ E&E fund custodian on or before the 10th day of the month following the period covered by the report and shall consist of the following:

10.8.e.(1). DCIS Form 75A;

10.8.e.(2). copy of monthly bank statement and DCIS Form 75A (Worksheet), E&E Account Reconciliation Worksheet (Attachment O), if applicable;

10.8.e.(3). DCIS Form 75, for each expenditure of E&E funds along with supporting documentation; and

10.8.e.(4). DCIS Form 74 and supporting documentation for funds that have been transferred into or out of the account from or to other DCIS E&E fund accounts.

10.8.f. The custodian of each account will prepare the monthly report and route it to the appropriate management officials for review and approval. After the monthly report for each E&E account has been approved by the approving official, all monthly reports and supporting documentation will be submitted electronically directly to the HQ E&E fund custodian. The

HQ E&E fund custodian is required to review each monthly report and provide summary information concerning the expenditure of E&E funds directly to the OIG Comptroller by the 15th calendar day of the month following the period covered by the reports. All completed monthly reports and claim forms will be marked “For Official Use Only/Law Enforcement Sensitive” (FOUO/LES) and protected accordingly.

10.9. Fund Administration

10.9.a. An E&E fund account is a “paper” account that is created to manage and account for the expenditure of E&E funds. An E&E account is comprised of one or more of the following components:

10.9.a.(1). cash-on-hand;

10.9.a.(2). bank account(s);

10.9.a.(3). pending advances (e.g., funds advanced, but not yet expended); and

10.9.a.(4). pending credits (e.g., credits posted to a covert credit card).

10.9.b. All of these components make up the E&E fund account and the balance of each component must be considered when reporting the “funds available” balance. The “funds available” balance reported on the DCIS Form 75 is the total of all cash-on-hand, bank account balances, pending advances, and pending credits that are associated with the subject E&E fund account.

10.9.c. In order to ensure operational effectiveness, each field office must establish and maintain at least one general E&E account. Additionally, a separate E&E account must be established for each approved Group I or Group II UCO for which a budget has been authorized. The purpose for establishing and maintaining separate E&E fund accounts is to prevent the commingling of general and UCO E&E expenses on the same E&E expense reports. Unless otherwise designated in writing, the main account will be the account that is physically maintained at the field office location.

10.9.d. The PD, SO will establish target funding levels for each of the main field office general E&E accounts. This target funding level will serve as a baseline for each account and is intended to ensure that sufficient funds are readily available in the field as well as to reduce the administrative burden associated with the submission, routing, approval, and filling of specific funding requests. When the target funding level for a specified E&E account drops below the established target, the HQ E&E fund custodian will notify the field office E&E custodian to submit a DCIS Form 74. The HQ E&E fund custodian will transfer the appropriate funds to bring the affected account up to the specified target funding level.

10.9.e. In the event that funds are needed in excess of the established target funding level, a specific request from or through the SAC, FO or ASAC must be submitted on DCIS

Form 74 to the PD, SO. The request should briefly explain why additional funds are required and indicate the method of funds transfer. The PD, SO and SAC, INV will review current E&E fund balances and projected expenditures against authorized funding targets established by the OIG Comptroller. If the request is approved, the HQ E&E fund custodian will transfer funds to the appropriate account.

10.9.f. Funds will be transferred to UCO E&E fund accounts on an “as needed” basis. Generally, requests for funds transfer should be based on anticipated expenditures and/or reasonable operational contingencies for the next 30-60 days. To obtain funds for a UCO E&E account, a specific request from or through the SAC, FO or ASAC must be submitted via e-mail to the UCO, PM. The request should be on a DCIS Form 74 with a brief explanation and method of funds transfer. The UCO, PM will review the request and ensure it is in line with the approved UCO budget. The UCO, PM will coordinate the request with the HQ E&E fund custodian to affect the transfer. Generally, coordination with the PD, SO is not necessary for UCO replenishments as UCO budgets are reviewed and approved by senior management officials prior to initiation or extension of the UCO. The UCO, PM and the HQ E&E fund custodian have the necessary visibility to (1) ensure the request complies with the approved UCO budget and (2) ensure that sufficient funds are available to meet the request. However, when E&E funds are restricted for dissemination, the PD, SO will advise the HQ E&E fund custodian and subsequent requests for UCO E&E replenishments will need to be coordinated with the PD, SO prior to disbursement of the funds.

10.9.g. Fund transfers between E&E accounts **must** be documented on a DCIS Form 74. No alias identification information will be entered on a DCIS Form 74, due to the potential compromise of identifying information. In such cases, the requester should indicate that the check be made payable to “a.k.a.” and the agent’s true identity. The alias identity will be obtained separately by the HQ E&E fund custodian. The “a.k.a.” should be redacted from the DCIS Form 74 when sent via FedEx with the check. Once the check is received, the recipient will execute the cash receipt portion of the DCIS Form 74 and return via e-mail to the HQ E&E fund custodian who will submit it along with the next monthly report.

10.9.h. DCIS was authorized to establish and maintain bank accounts relative to the administration of E&E funds. Therefore, bank accounts are authorized for the administration of E&E fund accounts. With exception of OCONUS accounts, no advances in excess of \$5,000 will be maintained in cash, unless there are compelling reasons to do so. In instances where a bank account has been determined to be appropriate, an e-mail notification must be forwarded to the HQ E&E fund custodian, with the name of the bank, the bank account number, and the DCIS representatives who have signature authority on that account in order to facilitate proper oversight of E&E fund accounts involving the use of bank accounts. The HQ E&E fund custodian will maintain this information in a central file, which will be available for inspection by auditors and appropriate management officials upon request. Additionally, the monthly bank statement **must** be included along with the monthly report. Bank accounts **must** be closed when no longer needed (e.g., after a UCO has been terminated) and an e-mail notification of the account closure **must** be sent to the HQ E&E fund custodian.

10.9.i. Under no circumstances will a check drawn on an overt account (e.g., an account held in the name of DCIS) be deposited to a covert account. Such transfers **must** be accomplished via sanitized check (e.g., alias check, certified check, or money order), cash, or Electronic Funds Transfer (EFT) (if such transaction conceals the name of the account from which the funds were drawn).

10.9.j. DCIS may not supplement its appropriations with interest earned from private financial institutions. Therefore, any interest earned will remain in the E&E account. Once the account has been closed, the interest will be returned to the U.S. Treasury. A check or money order payable to the U.S. Treasury will be forwarded to the HQ E&E fund custodian who will then forward the check to the OIG Comptroller. Due to the administrative burden associated with interest-bearing accounts, it is recommended that non-interest bearing accounts be established where appropriate.

10.9.k. SAC, FOs will ensure that all E&E account records, cash, and/or negotiable instruments are stored in an appropriate lockable container designated for the exclusive use of the E&E fund custodian. Only the primary and alternate custodians and the SAC, FO shall have access to the container. In the event that E&E funds are maintained in a subordinate office, the office supervisor will also have access to the container. If the container has a combination lock and is used to store cash or other negotiable instruments, the combination shall be changed at least annually and upon change of any person with knowledge of the container combination.

10.9.l. Fund custodians are authorized to advance funds to DCIS Special Agents and other third parties when deemed necessary and appropriate by management officials in advance of an anticipated expenditure. Advances should be made on as close as possible to the date the funds are needed and advances should generally be liquidated within one week of issuance, barring unforeseen operational circumstances. If not liquidated, the funds should be documented as pending advances. The funds must be approved in advance by the SAC, FO (or ASAC if authority has been formally delegated) and can be in the form of cash or other negotiable instrument, depending on mission requirements and security considerations.

10.9.m. To request an advance of funds, the requester will prepare a DCIS Form 74 and forward it through the appropriate chain of command (e.g., RAC, ASAC, and/or SAC FO) to obtain authorization of the approving official. When the requester is not located in the same office as the custodian, the preferred method for processing this request is via e-mail, and the e-mail string will serve as documentation of the approvals. Once approved, the DCIS Form 74 will be routed to the field office E&E fund custodian. The field office E&E fund custodian will advance the funds to the requestor. The requestor will sign the cash receipt portion of the DCIS Form 74 and the field office E&E fund custodian will track the funds in a "pending advance" status until the funds are expended or returned.

10.9.n. When the pending advances have been expended, the requestor will submit DCIS Form 75 with copies of receipts and other documentation as appropriate to the field office

E&E funds custodian. The field office E&E fund custodian will include the DCIS Form 75 as part of the monthly E&E report to HQ. A copy of the original DCIS Form 74 should be included with the monthly report.

10.9.o. Custodians must track and account for pending advances by maintaining a log containing, at a minimum, the following information:

10.9.o.(1). name and office code of the person to whom funds were advanced;

10.9.o.(2). date the funds were advanced;

10.9.o.(3). amount of advance;

10.9.o.(4). estimated liquidation date;

10.9.o.(5). actual date of liquidation; and

10.9.o.(6). breakdown of funds expended and funds returned.

The pending advance log should be maintained by fiscal year and in accordance with the E&E account record retention policy outlined in paragraph 10.9.x. below.

10.9.p. When cash that was originally obtained from E&E funds is no longer required to be maintained as evidence, it will be returned to the HQ E&E fund custodian by the evidence custodian. The HQ E&E fund custodian shall coordinate with the PD, SO and the OIG Comptroller for guidance on how to properly dispose of the funds. If the funds are from a prior fiscal year, the funds will be returned to the PD, SO in the form of a check or other negotiable instrument made payable to the U.S. Treasury. The PD, SO will forward the funds to the OIG Comptroller for return to the U.S. Treasury. **The OIG DoD cannot supplement its current fiscal year appropriation with funds from a prior fiscal year.**

10.9.q. Individuals entrusted with public funds specifically identified in this chapter as E&E funds are held personally accountable. Individuals are required to keep these funds safe, without loaning, using, or depositing them into personal banking accounts or exchanging them for other funds, except as specifically authorized by law and this regulation. Individuals are required to account for all amounts received or expended by producing evidence of the disposition of such funds at any given time. Should it be deemed necessary, DCIS HQ may recall E&E funds on demand. In the event that E&E funds cannot be produced by E&E fund custodians and/or DCIS personnel who are in receipt of an outstanding advance, or in the event that a loss of accountability has occurred, the correction/collection procedures outlined in section 10.11. below shall be implemented immediately.

10.9.r. Due to constant fluctuation in the exchange rates between U.S. dollars and foreign currencies, overseas offices shall retain copies of all receipts for the purchase of foreign currency. These receipts shall indicate the date of purchase, amount of U.S. dollars spent,

amount and type of the foreign currency received, and the rate of exchange. All expenditures involving foreign currency shall be recorded on all E&E documents in U.S. dollars and not in foreign currency.

10.9.s. When E&E funds need to be returned to the HQ E&E fund custodian, the funds will be returned using a check, money order, or EFT. All negotiable instruments will be made out to "DCIS," unless the funds (e.g., funds used to purchase evidence) relate to a prior fiscal year in which case the check will be made payable to the U.S. Treasury. The funds transfer will be accompanied by a DCIS Form 74 reflecting the HQ E&E fund custodian as the requester who will also sign and return the original to the appropriate field office E&E fund custodian.

10.9.t. Any advance approval of an expenditure that will be made from other than cash account balances (e.g., funds from other than the current fiscal year) requires the obligation of funds in the amount of the approved advance and must be coordinated with the OIG Comptroller. The PD, SO will conduct this coordination.

10.9.u. All E&E fund accounts must be reconciled monthly. Reconciliation of E&E accounts shall involve one or more of the following items:

10.9.u.(1). cash-on-hand,

10.9.u.(2). pending advances,

10.9.u.(3). bank balance, and/or

10.9.u.(4). receipts for expenditures.

The DCIS Form 75A contains a reconciliation worksheet for the basic components of an E&E fund account. Additionally, if the E&E fund account includes a bank account, the E&E fund custodian will complete a DCIS Form 75A (Worksheet), and the custodian will submit the completed worksheet with each monthly report. Note that the worksheet contains a section to report claimed expenses for which funds have not yet been expended. In most instances, expenses will not be claimed until funds have actually been expended. However, travel expenses will be claimed as of the date the voucher is reviewed and approved by management. In such cases, it may be likely that the funds related to such expenses have not yet been expended due to timing differences between credit card bills and the date the travel voucher has been reviewed and approved by management.

10.9.v. The total of the above items shall always equal the amount of the funds that have been provided to the E&E fund custodian. The reconciliation worksheet contained within the DCIS Form 75A must be used to facilitate and record the reconciliation process. All E&E fund custodians shall reconcile their E&E fund accounts at least monthly and must maintain either a hardbound ledger book or the use of Money, Quicken, or other similar financial management software package to track and account for E&E funds. All information must be properly safeguarded as FOUO/LES information and backed up regularly.

10.9.w. Title 10, U.S.C., § 127, provides that "...the Secretary of Defense shall submit a report of such expenditures on a quarterly basis..." to Congress. Information provided in monthly E&E fund reports is provided to the OIG Comptroller who in turn relies on this information in reporting E&E fund expenditures to the DoD Comptroller. The DoD Comptroller reports this information to the Secretary of Defense, who ultimately reports the information to Congress. Therefore, it is imperative that E&E fund custodians ensure accurate and timely reporting of E&E fund expenditures on their monthly reports.

10.9.x. The E&E records maintained in the field are considered working copies of the official records, which are submitted to DCIS HQ by the 10th calendar day of each month following the period covered. For all E&E accounts, including general and UCO accounts, copies of all monthly reports and all supporting documentation must be retained in the field office for 6 years, 3 months, before they can be destroyed locally after the close of the fiscal year.

10.10. Inspection and Audit

10.10.a. Claims for E&E expenses will be reviewed and approved by the first line supervisor and the appropriate approving official (e.g., SAC, FO) for the purpose of verifying that all expenses were appropriate, properly documented, and made in accordance with established policy, prior to submission to the HQ E&E fund custodian. Additionally, all claims shall be reviewed by the SAC, INV and the HQ E&E fund custodian for the purpose of ensuring completeness and accuracy. The HQ E&E fund custodian will provide the OIG Comptroller with copies of all reports on a monthly basis for audit.

10.10.b. The SAC, FOs; ASAC; or their designee shall conduct at least one surprise audit of E&E accounts per fiscal year and must maintain a record of such audits, which *must* be forwarded to the HQ E&E fund custodian. At a minimum, the surprise audits should involve a reconciliation of at least one monthly report for each active E&E fund account. Additionally, the overall management and oversight of E&E funds shall be thoroughly examined during the regular inspection of each field office. Annual inspections of field office E&E accounts will be conducted by the PD, SO or his/her designee, along with the OIG Comptroller. The combination of one surprise audit, along with the annual inspection by HQ will meet DCIS policy requirements of two inspections per fiscal year. In the event that HQ is unable to conduct its annual inspection, a second surprise audit by the SAC, FOs; ASAC; or their designee will suffice to meet policy requirements.

10.11. Correction/Collection Procedures

10.11.a. Every effort should be made to avoid erroneous reporting. In the event that an error is detected after the approving official has approved the monthly report, the error will immediately be brought to the attention of the approving official. The approving official will promptly notify the HQ E&E fund custodian of the suspected error. The approving official will investigate the reported error and determine the nature and extent of the error. The approving

official will submit a corrected monthly report and supporting documentation to the HQ E&E fund custodian, along with a narrative explanation reporting the details of the error and any corrective action taken.

10.11.b. Improper expenditures are those that, at some point in the administrative process, are determined to be not chargeable to the E&E expense budget line item. This determination may be made by any of the officials normally involved in the E&E fund administrative chain, including the OIG Comptroller. All improper expenditures and claims must be corrected, whether by collection or reclassification.

10.11.b.(1). Expenditures that are determined to be not allowable under the E&E fund budget line item, but are properly chargeable to another OIG DoD budget line item, will be corrected by submission of an SF-1164 and the claimant will reimburse the appropriate E&E fund custodian for the amount of the erroneous claim.

10.11.b.(2). Expenditures that are not properly chargeable to any OIG DoD appropriation will be disallowed. If a claim is paid and charged to the E&E expense budget line item and is subsequently determined to be not chargeable to any OIG DoD appropriation, then the individual(s) submitting and/or authorizing the original claim will assume personal liability for the expense. Reimbursement will be obtained as soon as possible (normally within 72 hours of identification and determination of the impropriety), utilizing the individual's personal funds. The appropriate E&E fund custodian will collect the funds, correct the affected monthly report, and provide the original claimant with a receipt reflecting the date, amount, and purpose for which the funds were collected. The affected fund custodian will then forward the corrected monthly report and a copy of the receipt that was provided to the claimant to the appropriate approving official, who then forwards the package to the HQ E&E fund custodian.

10.11.c. In situations where a fiscal irregularity has occurred resulting in a loss of accountability, the Commander shall take the following actions in accordance with the principles outlined in the DoD FMR, Volume 5, Chapter 6, "Physical Losses of Funds, Erroneous Payments, and Overages—Information for Investigating Officer" (Attachment M).

10.11.c.(1). Promptly notify the PD, SO and the SAC, INV.

10.11.c.(2). Appoint an investigating officer who is familiar with investigative techniques and has knowledge of the required internal controls, pertinent laws, and directives. The investigating officer should be of equal or higher grade than the accountable individuals involved in the fiscal irregularity and, ideally, should not be in the same chain of command as the accountable individuals. The investigating officer will be required to collect and report in writing the following information.

10.11.c.(2).(a). The identities of all accountable individuals who are pecuniarily liable for the loss, their Social Security numbers, the amount for which each is accountable, and the involvement of each in the loss.

10.11.c.(2).(b). The circumstances leading to and surrounding the loss and the efforts undertaken to discover the cause of a loss that remains unexplained.

10.11.c.(2).(c). The description of the internal controls prescribed to prevent losses of the type experienced and the steps taken to implement those controls.

10.11.c.(2).(d). Other relevant information that would aid in understanding how the loss occurred and in evaluating whether relief is appropriate for the accountable individuals involved.

10.11.c.(2).(e). Appropriate documentary evidence to support information reported to the Commander.

10.11.c.(3). Review the written report of the investigating officer and render in writing the following findings and recommendations.

10.11.c.(3).(a). A finding as to whether or not there was a loss to the U.S. Government.

10.11.c.(3).(b). A finding as to the amount of the loss, if applicable.

10.11.c.(3).(c). A finding as to whether the loss is a physical loss or one that involves fraud.

10.11.c.(3).(d). A finding as to whether or not the accountable individual was acting in the line of duty with respect to the loss.

10.11.c.(3).(e). A finding as to whether the loss was due to the fault or negligence of the accountable official. A separate finding shall be made for each accountable individual involved.

10.11.c.(3).(f). A recommendation as to whether or not the accountable individual should be relieved of pecuniary liability for the loss. Provide separate recommendations concerning each accountable individual involved.

10.11.c.(3).(g). A recommendation as to appropriate corrective action(s) for improving controls or procedures, if applicable.

10.11.c.(3).(h). Any other recommendations that are appropriate, considering the facts that were developed during the course of the investigation.

10.11.c.(4). In cases where criminal impropriety appears to exist, the Commander will promptly notify the SAC, INV and the AIGI-INV.

10.11.d. Requests for relief of personal liability, when such is indicated, will be submitted in accordance with the DoD FMR.

10.11.e. Repetitive instances of improper claims by an office or individual will be researched for cause and, if necessary, corrective measures will be initiated that provide reasonable assurance future discrepancies will not occur.

ATTACHMENTS

<u>Attachment</u>	<u>Title</u>
A	Title 10 U.S.C. 127, Emergency and Extraordinary Expenses
B	Memorandum, dated February 28, 2011, from the Inspector General to the Deputy Inspector General for Investigations, delegating approval authority for E&E expenditures
C	Memorandum, dated April 7, 2011, from the Deputy Inspector General for Investigations to Special Agents in Charge, delegating approval authority for E&E expenditures
D	DoD Instruction 7000.14, DoD Financial Management Regulation (FMR), September 17, 2008
E	Memorandum, dated December 23, 1996, from the DoD Comptroller granting DCIS authority to establish and maintain bank accounts
F	DCIS Form 75, Claim for E&E Expense
G	DCIS Form 74, Request for Advance of E&E Funds
H	DCIS Form 8C, Confidential Informant Payment Request <i>[under development]</i>
I	DCIS Form 8D, Confidential Informant Payment Receipt <i>[under development]</i>
J	DD Form 1351-2, Travel Voucher or Subvoucher
K	DD Form 1351-3, Statement of Actual Expenses
L	SF Form 1164, Claim for Reimbursement for Expenditures on Official Business
M	DoD Regulation 7000.14-R, Volume 5, Chapter 6, July 2009, Physical Losses of Funds, Erroneous Payments and Overages – Information for Investigating Officer
N	DCIS Form 75A, Monthly Summary Report
O	DCIS Form 75A (Worksheet), E&E Account Reconciliation Worksheet

ATTACHMENT A

TITLE 10, UNITED STATES CODE, SECTION 127, EMERGENCY AND EXTRAORDINARY EXPENSES

TITLE 10 - ARMED FORCES

Subtitle A - General Military Law

PART I - ORGANIZATION AND GENERAL MILITARY POWERS

CHAPTER 3 - GENERAL POWERS AND FUNCTIONS

-HEAD-

Sec. 127. Emergency and extraordinary expenses

-STATUTE-

(a) Subject to the limitations of subsection (c), and within the limitation of appropriations made for the purpose, the Secretary of Defense, the Inspector General of the Department of Defense, and the Secretary of a military department within his department, may provide for any emergency or extraordinary expense which cannot be anticipated or classified. When it is so provided in such an appropriation, the funds may be spent on approval or authority of the Secretary concerned or the Inspector General for any purpose he determines to be proper, and such a determination is final and conclusive upon the accounting officers of the United States. The Secretary concerned or the Inspector General may certify the amount of any such expenditure authorized by him that he considers advisable not to specify, and his certificate is sufficient voucher for the expenditure of that amount.

(b) The authority conferred by this section may be delegated by the Secretary of Defense to any person in the Department of Defense, by the Inspector General to any person in the Office of the Inspector General, or by the Secretary of a military department to any person within his department, with or without the authority to make successive redelegations.

(c)(1) Funds may not be obligated or expended in an amount in excess of \$500,000 under the authority of subsection (a) or (b) until the Secretary of Defense has notified the Committee on Armed Services and the Committee on Appropriations of the Senate and the Committee on Armed Services and the Committee on Appropriations of the House of Representatives of the intent to obligate or expend the funds, and -

(A) in the case of an obligation or expenditure in excess of \$1,000,000, 15 days have elapsed since the date of the notification; or

(B) in the case of an obligation or expenditure in excess of \$500,000, but not in excess of \$1,000,000, 5 days have elapsed since the date of the notification.

(2) Subparagraph (A) or (B) of paragraph (1) shall not apply to an obligation or expenditure of funds otherwise covered by such subparagraph if the Secretary of Defense determines that the national security objectives of the United States will be compromised by the application of the subparagraph to the obligation or expenditure. If the Secretary makes a determination with respect to an obligation or expenditure under the preceding sentence, the Secretary shall immediately notify the committees referred to in paragraph (1) that such obligation or expenditure is necessary and provide any relevant information (in classified form, if necessary) jointly to the chairman and ranking minority member (or their designees) of such committees.

(3) A notification under paragraph (1) and information referred to in paragraph (2) shall include the amount to be obligated or expended, as the case may be, and the purpose of the obligation or expenditure.

(d) Annual Report. - Not later than December 1 each year, the Secretary of Defense shall submit to the congressional defense committees a report on expenditures during the preceding fiscal year under subsections (a) and (b).

-SOURCE-

(Added Pub. L. 94-106, title VIII, Sec. 804(a), Oct. 7, 1975, 89 Stat. 538, Sec. 140; amended Pub. L. 98-94, title XII, Sec. 1268(2), Sept. 24, 1983, 97 Stat. 705; renumbered Sec. 127 and amended Pub. L. 99-433, title I, Secs. 101(a)(3), 110(d)(4), Oct. 1, 1986, 100 Stat. 994, 1002; Pub. L. 103-160, div. A, title III, Sec. 361, Nov. 30, 1993, 107 Stat. 1627; Pub. L. 103-337, div. A, title III, Sec. 378, Oct. 5, 1994, 108 Stat. 2737; Pub. L. 104-106, div. A, title IX, Sec. 915, title XV, Sec. 1502(a)(5), Feb. 10, 1996, 110 Stat. 413, 502; Pub. L. 106-65, div. A, title X, Sec. 1067(1), Oct. 5, 1999, 113 Stat. 774; Pub. L. 108-136, div. A, title X, Sec. 1031(a)(2), Nov. 24, 2003, 117 Stat. 1596.)

-MISC1-

AMENDMENTS

2003 - Subsec. (d). Pub. L. 108-136 amended subsec. (d) generally. Prior to amendment, subsec. (d) read as follows: "In any case in which funds are expended under the authority of subsections (a) and (b), the Secretary of Defense shall submit a report of such

expenditures on a quarterly basis to the Committee on Armed Services and the Committee on Appropriations of the Senate and the Committee on Armed Services and the Committee on Appropriations of the House of Representatives."

1999 - Subsecs. (c)(1), (d). Pub. L. 106-65 substituted "and the Committee on Armed Services" for "and the Committee on National Security".

1996 - Subsec. (c). Pub. L. 104-106, Sec. 915(2), added subsec. (c). Former subsec. (c) redesignated (d).

Pub. L. 104-106, Sec. 1502(a)(5), substituted "Committee on Armed Services and the Committee on Appropriations of the Senate and the Committee on National Security and the Committee on Appropriations of" for "Committees on Armed Services and Appropriations of the Senate and".

Subsec. (d). Pub. L. 104-106, Sec. 915(1), redesignated subsec. (c), as amended by Pub. L. 104-106, Secs. 1502(a)(5), 1506, as (d).

1994 - Subsec. (c). Pub. L. 103-337 struck out par. (1) designation before "In any case" and struck out par. (2) which read as follows: "The amount of funds expended by the Inspector General of the Department of Defense under subsections (a) and (b) during a fiscal year may not exceed \$400,000."

1993 - Subsec. (a). Pub. L. 103-160, Sec. 361(1), inserted ", the Inspector General of the Department of Defense," after "the Secretary of Defense" and "or the Inspector General" after "the Secretary concerned" and after "The Secretary concerned".

Subsec. (b). Pub. L. 103-160, Sec. 361(2), inserted ", by the Inspector General to any person in the Office of the Inspector General," after "the Department of Defense".

Subsec. (c). Pub. L. 103-160, Sec. 361(3), designated existing provisions as par. (1) and added par. (2).

1986 - Pub. L. 99-433 renumbered section 140 of this title as this section and substituted "Emergency" for "Emergencies" in section catchline.

1983 - Subsec. (a). Pub. L. 98-94 struck out "of this section" after "subsection (c)".

Subsec. (c). Pub. L. 98-94 struck out "of this section" after "subsections (a) and (b)".

CONSTRUCTION AUTHORITY OF SECRETARY OF DEFENSE UNDER DECLARATION OF

WAR OR NATIONAL EMERGENCY

Pub. L. 97-99, title IX, Sec. 903, Dec. 23, 1981, 95 Stat. 1382, which authorized the Secretary of Defense, in the event of a declaration of war or the declaration of a national emergency by the President, to undertake military construction without regard to

any other provisions of law, was repealed and restated as section 2808 of this title by Pub. L. 97-214, Secs. 2(a), 7(18), July 12, 1982, 96 Stat. 157, 174, effective Oct. 1, 1982.

ATTACHMENT B



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

FEB 28 2011

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR INVESTIGATIONS

SUBJECT: Delegation of Emergency and Extraordinary Expense Approval Authority

Pursuant to Title 10, United States Code, Section 127 (10 U.S.C. §127), "Emergency and Extraordinary expenses," and subject to the limitations set forth below, I hereby delegate to you authority to approve Emergency and Extraordinary (E&E) expenditures as follows:


- You are authorized to approve E&E expenditures up to the current fiscal year expense target, as established and modified by the Comptroller, and subject to the availability of funds. Written concurrence from the Comptroller is required for the approval of any amount above the current cash-on-hand amount maintained within Defense Criminal Investigative Service (DCIS) E&E accounts.
- You may further delegate E&E expenditure approval authority in writing, and you may authorize your delegates to further delegate E&E expenditure approval authority in writing. Under no circumstances shall E&E expenditure approval authority be delegated below the Assistant Special Agents in Charge level. All such delegations shall contain the limitations set forth below.

All personnel to whom approval authority is delegated shall execute a DD Form 577, Appointment/Termination Record - Authorized Signature (Attachment), prior to approving any expenditure of E&E funds.

All DCIS personnel shall follow the requirements set forth in Chapter 10 of the DCIS Special Agents Manual (SAM) regarding the use and administration of E&E funds.

Before approving any E&E expenditures not specifically authorized by Chapter 10 of the SAM, the E&E Approving Official shall obtain a written legal opinion from the Office of General Counsel.

All E&E approving officials shall be personally liable for funds expended pursuant to their approval in the event such expenditure is later determined to be contrary to law or regulation.


Gordon S. Heddell

Attachment:
As stated

cc:
OIG Comptroller

ATTACHMENT C



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

APR - 7 2011

(Investigations)

MEMORANDUM FOR SPECIAL AGENTS IN CHARGE

SUBJECT: Delegation of Emergency and Extraordinary Expense Approval Authority

Pursuant to 10 U.S.C. §127, "Emergency and extraordinary expenses," and subject to the limitations set forth below, I hereby delegate to you authority to approve Emergency and Extraordinary (E&E) expenditures as follows:

- o You are authorized to approve E&E expenditures up to \$5,000, subject to the availability of funds. Expenditures exceeding \$5,000 require approval from the Special Agent in Charge, Investigative Operations. Expenditures exceeding \$10,000 require approval from the Deputy Inspector General for Investigations.
- o You may further delegate E&E expenditure approval authority in writing, and you may authorize your delegates to further delegate E&E expenditure approval authority in writing. Under no circumstances shall E&E expenditure approval authority be delegated below the Assistant Special Agents in Charge level. All such delegations shall contain the limitations set forth below.

All personnel to whom approval authority is delegated shall execute a DD Form 577, Appointment/Termination Record - Authorized Signature (attached), prior to approving any expenditure of E&E funds.

All DCIS personnel shall follow the requirements set forth in Chapter 10 of the DCIS Special Agents Manual (SAM) regarding the use and administration of E&E funds. Before approving any E&E expenditures not specifically authorized by Chapter 10 of the SAM, the E&E Approving Official shall obtain a written legal opinion from the Office of General Counsel.

All E&E approving officials shall be personally liable for funds expended pursuant to their approval in the event such expenditure is later determined to be contrary to law or regulation.

James B. Burch
Deputy Inspector General
for Investigations

Attachment:
As stated

cc:
OTG Comptroller

ATTACHMENT E



COMPTROLLER

OFFICE OF THE UNDER SECRETARY OF DEFENSE
1100 DEFENSE PENTAGON
WASHINGTON, DC 20301-1100



SEC 2.3 1996

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

SUBJECT: Request for Exception to Elimination of Imprest Funds

Your memorandum of September 27, 1996, on this subject, requested exception to the policy that eliminated imprest funds for specific purposes within your Office of the Assistant Inspector General for Investigations. The specific purposes are designated for emergency and extraordinary (E&E) accounts at the Headquarters and six field locations: Philadelphia, PA; Arlington, VA; Atlanta, GA; Los Angeles, CA; St. Louis, MO; and Dallas, TX.

Since receipt of your request, this office has worked closely with representatives of your Investigations office to determine the best approach for operating such accounts. It now is understood that your office, in cooperation with the Defense Finance and Accounting Service (DFAS)-Indianapolis Center, has decided to administer the accounts through Disbursing Officer (DO) Paying Agents, as authorized by paragraph 020604, "Paying Agents," in Volume 5, "Disbursing Policy and Procedures," of the DoD Financial Management Regulation.

Consequently, you are authorized to establish Paying Agents and maintain funds explicitly for the E&E purposes cited in your request. Funds held always should be kept to the minimum essential requirement, preferably not to exceed the amount needed for one month and, where practical and economically justified, should be maintained in an interest bearing account at each location.

Please continue to work with the DFAS to effect this process by March 31, 1997. My staff contact for this matter is (b)(6), (b)(7)(C). He may be reached at (703) 6975, (b)(7)(D&N 2375), (b)(7) or e-mail address: (b)(7)@ousdc.osd.mil.

Alvin Tucker
Deputy Chief Financial Officer

cc: DFAS-HQ/F
DFAS-HQ/C

ATTACHMENT F

CLAIM FOR E&E EXPENSES

PRINTED/TYPED NAME OF CLAIMANT: _____
OFFICE CODE: _____ PERIOD COVERED: _____ TO _____

ITEMIZED EXPENSES:

DATE	DESCRIPTION	UID	CATEGORY	UCO LINE ITEM	AMOUNT
Total from continuation pages					

TOTAL AMOUNT CLAIMED:

Page 1 of

CERTIFICATION:

The above information is true and correct and in compliance with DCIS SAM Chapter 10. Original receipts have been attached for all expenditures in excess of \$75. Where receipts were not available, a Memorandum for Record has been attached fully identifying the nature of the expense and the reason why no receipt was available.

Claimant Signature

Date

I have reviewed the claimed expenses and I have determined that they have been properly documented, were incurred in connection with official business, and are proper for payment in accordance with DCIS SAM Chapter 10.

Supervisor's Printed Name

Supervisor's Signature

Date

I have approved the claimed expenses in accordance with DCIS SAM Chapter 10.

Approving Official's Printed Name

Approving Official's Signature

Date

DCIS Form 75 (Jan 2004)
Law Enforcement Sensitive (when filled in)

ATTACHMENT G

REQUEST FOR ADVANCE OF E&E FUNDS

REQUESTOR: _____ TITLE: _____

OFFICE: _____ PHONE: _____

ADDRESS: _____

AMOUNT REQUESTED: _____ DATE OF REQUEST: 6/28/2011

PURPOSE: _____

METHOD OF ADVANCE (check one):

☐ Cash (justify): _____

☐ EFT: (routing number/bank account): _____

☐ Check (payable to): _____

☐ Certified Funds/Money Order (payable to): _____

*****NOTE: DO NOT LIST ALIAS NAMES ON THIS FORM*****

Requestor's Signature

Approving Official's Signature

(Detach this portion and return to sender)

CASH RECEIPT CERTIFICATE

RECEIVED FROM: _____ TITLE: _____

OFFICE: _____ PHONE: _____

AMOUNT RECEIVED: _____

I acknowledge that I am strictly liable to the United States for all public funds under my control. I have read and understand Chapter 10, DCIS Special Agent's Manual regarding the expenditure of E&E funds.

Printed Name

Signature

Date

ATTACHMENT J

TRAVEL VOUCHER OR SUBVOUCHER				Read Privacy Act Statement, Penalty Statement, and instructions on back before completing form. Use typewriter, ink, or ball point pen. PRESS HARD. DO NOT use pencil. If more space is needed, continue on remarks.			
1. PAYMENT <input type="checkbox"/> Electronic Fund Transfer (EFT) <input type="checkbox"/> Payment by Check		3. SPLIT DISBURSEMENT: The Paying Office will pay directly to the Government Travel Charge Card (GTCC) contractor the portion of your reimbursement representing travel charges for transportation, lodging, and rental car if you are a civilian employee, unless you elect a different amount. Military personnel are required to designate a payment that equals the total of their outstanding government travel card balance to the GTCC contractor. Pay the following amount of this reimbursement directly to the Government Travel Charge Card contractor: \$					
2. NAME (Last, First, Middle Initial) (Print or type)		3. GRADE		4. SSN		5. TYPE OF PAYMENT (X as applicable) <input type="checkbox"/> TDY <input type="checkbox"/> Member/Employee <input type="checkbox"/> PCS <input type="checkbox"/> Other <input type="checkbox"/> Dependent(s) <input type="checkbox"/> DLA	
6. ADDRESS: a. NUMBER AND STREET		b. CITY		c. STATE		d. ZIP CODE	
a. E-MAIL ADDRESS		7. DAYTIME TELEPHONE NUMBER & AREA CODE		8. TRAVEL ORDER AUTHORIZATION NUMBER		9. PREVIOUS GOVERNMENT PAYMENTS/ADVANCES	
11. ORGANIZATION AND STATION		12. DEPENDENT(S) (X and complete as applicable) <input type="checkbox"/> ACCOMPANIED <input type="checkbox"/> UNACCOMPANIED a. NAME (Last, First, Middle Initial) b. RELATIONSHIP c. DATE OF BIRTH OR MARRIAGE		13. DEPENDENT'S ADDRESS ON RECEIPT OF ORDERS (Include Zip Code)		10. FOR D.O. USE ONLY a. D.O. VOUCHER NUMBER b. SUBVOUCHER NUMBER c. PAID BY	
14. HAVE HOUSEHOLD GOODS BEEN SHIPPED? (X one) <input type="checkbox"/> YES <input type="checkbox"/> NO (Explain in Remarks)		15. ITINERARY a. DATE b. PLACE (Home, Office, Base, Activity, City and State, City and Country, etc.)		c. MEANS/ MODE OF TRAVEL		d. REASON FOR STOP	
e. LODGING COST		f. POC MILES		g. SUMMARY OF PAYMENT (1) Per Diem (2) Actual Expense Allowance (3) Mileage (4) Dependent Travel (5) DLA (6) Reimbursable Expenses (7) Total (8) Less Advance (9) Amount Owed (10) Amount Due			
16. POC TRAVEL (X one) <input type="checkbox"/> OWN/OPERATE <input type="checkbox"/> PASSENGER		17. DURATION OF TRAVEL 12 HOURS OR LESS MORE THAN 12 HOURS BUT 24 HOURS OR LESS MORE THAN 24 HOURS		18. GOVERNMENT DEDUCTIBLE MEALS a. DATE b. NO. OF MEALS c. DATE d. NO. OF MEALS			
19. REIMBURSABLE EXPENSES a. DATE b. NATURE OF EXPENSE c. AMOUNT d. ALLOWED		20. CLAIMANT SIGNATURE		b. DATE			
c. REVIEWER'S PRINTED NAME		d. REVIEWER SIGNATURE		a. TELEPHONE NUMBER		f. DATE	
21. APPROVING OFFICIAL'S PRINTED NAME		b. SIGNATURE		c. TELEPHONE NUMBER		d. DATE	
22. ACCOUNTING CLASSIFICATION							
23. COLLECTION DATA							
24. COMPUTED BY		25. AUDITED BY		26. TRAVEL ORDER AUTHORIZATION POSTED BY		27. RECEIVED (Payee Signature and Date or Check No.)	
28. AMOUNT PAID							

DD FORM 1351-2, MAR 2008

PREVIOUS EDITION MAY BE USED UNTIL SUPPLY IS EXHAUSTED.

Exception to SF 1012 approved by GSAR/MS 12-01. Adobe Designer 7.0

PRIVACY ACT STATEMENT

AUTHORITY: 5 U.S.C. Section 5701, 37 U.S.C. Sections 404 - 427, 5 U.S.C. Section 301, DoDFMR 7000.14-R, Vol. 9, and E.O. 9397.

PRINCIPAL PURPOSE(S): This record is used for reviewing, approving, accounting, and disbursing money for claims submitted by Department of Defense (DoD) travelers for official Government travel. The Social Security number (SSN) is used to maintain a numerical identification filing system for filing and retrieving individual claims.

ROUTINE USE(S): Disclosures are permitted under 5 U.S.C. 552a(b), Privacy Act of 1974, as amended. In addition, information may be disclosed to the Internal Revenue Service for travel allowances, which are subject to Federal income taxes, and for any DoD "Blanket Routine Use" as published in the Federal Register.

DISCLOSURE: Voluntary; however, failure to furnish the information requested may result in total or partial denial of the amount claimed.

PENALTY STATEMENT

There are severe criminal and civil penalties for knowingly submitting a false, fictitious, or fraudulent claim (U.S. Code, Title 18, Sections 287 and 1001 and Title 31, Section 3729).

INSTRUCTIONS

ITEM 1 - PAYMENT

Member must be on electronic funds (EFT) to participate in split disbursement. Split disbursement is a payment method by which you may elect to pay your official travel card bill and forward the remaining settlement dollars to your predesignated account. For example, \$250.00 in the "Amount to Government Travel Charge Card" block means that \$250.00 of your travel settlement will be electronically sent to the charge card company. Any dollars remaining on this settlement will automatically be sent to your predesignated account. Should you elect to send more dollars than you are entitled, "all" of the settlement will be forwarded to the charge card company. Notification: you will receive your regular monthly billing statement from the Government Travel Charge Card contractor; it will state: paid by Government, \$250.00, 0 due. If you forwarded less dollars than you owe, the statement will read as: paid by Government, \$250.00, \$15.00 now due. Payment by check is made to travelers only when EFT payment is not directed.

REQUIRED ATTACHMENTS

1. Original and/or copies of all travel orders/authorizations and amendments, as applicable.
2. Two copies of dependent travel authorization if issued.
3. Copies of secretarial approval of travel if claim concerns parents who either did not reside in your household before their travel and/or will not reside in your household after travel.
4. Copy of GTR, MTA or ticket used.
5. Hotel/motel receipts and any item of expense claimed in an amount of \$75.00 or more.
6. Other attachments will be as directed.

ITEM 15 - ITINERARY - SYMBOLS

15c. MEANS/MODE OF TRAVEL (Use two letters)

GTR/TKT or CBA (See Note)	- T	Automobile	- A
Government Transportation	- G	Motorcycle	- M
Commercial Transportation		Bus	- B
(Own expense)	- C	Plane	- P
Privately Owned		Rail	- R
Conveyance (POC)	- P	Vessel	- V

Note: Transportation tickets purchased with a CBA must not be claimed in Item 18 as a reimbursable expense.

15d. REASON FOR STOP

Authorized Delay	- AD	Leave En Route	- LV
Authorized Return	- AR	Mission Complete	- MC
Awaiting Transportation	- AT	Temporary Duty	- TD
Hospital Admittance	- HA	Voluntary Return	- VR
Hospital Discharge	- HD		

ITEM 15e. LODGING COST

Enter the total cost for lodging.

ITEM 19 - DEDUCTIBLE MEALS

Meals consumed by a member/employee when furnished with or without charge incident to an official assignment by sources other than a government mess (see JFTR, par. U4125-A3g and JTR, par. C4554-B for definition of deductible meals). Meals furnished on commercial aircraft or by private individuals are not considered deductible meals.

28. REMARKS

a. INDICATE DATES ON WHICH LEAVE WAS TAKEN:

b. ALL UNUSED TICKETS (including identification of unused "e-tickets") MUST BE TURNED IN TO THE T/O OR CTO.

STATEMENT OF ACTUAL EXPENSES

[illegible]

CLAIM FOR REIMBURSEMENT FOR EXPENDITURES ON OFFICIAL BUSINESS

DoD Overprint 4/2002

STANDARD FORM 1164 (Rev. 11-77)
Prescribed by GSA, FPMR (41 CFR) 101-7

CLAIM FOR REIMBURSEMENT FOR EXPENDITURES ON OFFICIAL BUSINESS

DoD Overprint 4/2002

STANDARD FORM 1164 (Rev. 11-77)
Prescribed by GSA, FPMR (CPR 41) 101-7

In compliance with the Privacy Act of 1974, the following information is provided: Solicitation of the information on this form is authorized by 5 U.S.C. Chapter 57 as implemented by the Federal Travel Regulations (FPMR 101-7), E.O. 11609 of July 22 1971, E.O. 11012 of March 27, 1962, E.O. 9397 of November 22, 1943, and 5 U.S.C. 6011(b) and 6109. The primary purpose of the requested information is to determine payment or reimbursement to eligible individuals for allowable travel and other expenses incurred under appropriate administrative authorization and to record and maintain costs of such reimbursements to the Government. The information will be used by Federal agency officers and employees who have a need for the information in the performance of their official duties. The information may be disclosed to appropriate Federal, State, local, or foreign agencies, when relevant to civil, criminal, or regulatory investigations or prosecutions, or when pursuant to a requirement by this agency in connection with the hiring or firing of an employee, the issuance of a security clearance, or investigations of the performance of official duties. This information is requested pursuant to 5 U.S.C. 6011(b) and 6109, E.O. 11609 of July 22 1971, E.O. 11012 of March 27, 1962, E.O. 9397 of November 22, 1943, for use as taxpayer and/or employee identification number; disclosure is MANDATORY on vouchers claiming payment or reimbursement which is, or may be, taxable income. Disclosure of your SSN and other requested information is voluntary in all other instances; however, failure to provide the information (other than SSN) required to support the claim may result in delay or loss of reimbursement.

**SUMMARY OF MAJOR CHANGES TO
DoD 7000.14-R, VOLUME 5, CHAPTER 6
“PHYSICAL LOSSES OF FUNDS, ERRONEOUS PAYMENTS,
AND OVERAGES”**

All changes are denoted in blue font.

Substantive revisions are denoted by a ★ preceding the section,
paragraph, table, or figure that includes the revision.

Hyperlinks are denoted by *underlined, bold, italic, blue font*

PARAGRAPH	EXPLANATION OF CHANGE/REVISION	PURPOSE
All	Revises entire chapter to include renaming the chapter, rewriting and renumbering paragraphs. Relabeled and renumbered figures and tables at the end of the chapter. Updates addresses throughout the chapter.	Update

★TABLE OF CONTENTS**PHYSICAL LOSSES OF FUNDS, ERRONEOUS PAYMENTS, AND OVERAGES**

0601	Physical Losses of Funds
0602	Erroneous Payments (Illegal, Incorrect, and Improper Payments)
0603	Decisions on Liability
0604	Overages of Public Funds
Figure 6-1	Department of Defense (DD) Form 2667, “Subsidiary Accountability Record” (Cumulative Physical Losses of Funds)
Figure 6-2	Minor Physical Losses – No Fraud
Figure 6-3	Request for Extension of Investigation
Figure 6-4	Erroneous Payments – No Fraud
Figure 6-5	DD Form 2667, “Subsidiary Accountability Record” (Overage of Funds Record)
Table 6-1	Physical Loss of Funds Examples
Table 6-2	Processing Physical Losses of Funds
Table 6-3	Processing Change Fund or Imprest Fund Loss
Table 6-4	Questions to Use for Investigations
Table 6-5	Examples of Erroneous Payments Requiring an Investigation and Payments Not Requiring an Investigation
Table 6-6	Processing Erroneous Payments

CHAPTER 6

PHYSICAL LOSSES OF FUNDS, ERRONEOUS PAYMENTS, AND OVERAGES

0601 PHYSICAL LOSSES OF FUNDS. Examples of physical losses of funds are provided in Table 6-1.

060101. Minor. Loss of less than \$750 without any evidence of fraud within the disbursing office.

060102. Major

A. Loss of \$750 or more.

B. Any loss, regardless of the dollar amount, resulting from a theft.

C. Any loss, regardless of the dollar amount, where there is evidence of fraud within the disbursing office; e.g., embezzlement, or fraudulent acts of disbursing personnel, acting alone or in collusion with others.

060103. Discovery of Loss

A. General. Any person who believes that an individual entrusted with public funds is misusing those funds shall notify the commander having jurisdiction over the alleged offender of the alleged misuse. See Table 6-2 for an overview of processing physical losses of funds.

B. Disbursing Officer (DO) Responsibilities

1. Verify that all transactions have been properly posted (e.g., Daily Statement of Accountability (*Department of Defense (DD) Form 2657*), Daily Agent Accountability Summary (*DD Form 2665*)).

2. Verify the accuracy of all totals since the date of last balancing on the DD Form 2657 and each deputy's, agent's, or cashier's DD Form 2665.

3. Verify by actual count that the total of all cash and documents held as cash by the DO and all deputies, agents, and cashiers is in agreement with the amount shown as being on hand on the DD Forms 2657 and 2665.

4. If the loss is not resolved within 24 hours of discovery and is a major physical loss as defined in paragraph 060102 of this chapter or is the result of suspected fraud, then report the loss in writing to the commander.

5. Request that the commander direct an immediate audit of all disbursing assets by a Cash Verification Team to confirm that a loss has occurred.

C. Commander's Responsibilities. Upon notification of a possible loss, request the Cash Verification Team conduct an audit of the DO's account. If the discrepancy is not resolved and is a major loss of funds as described in paragraph 060102 of this chapter or is the result of a payment due to fraud, then report through the chain of command within 24 hours via email to Disbursing-DebtManagementPolicy@DFAS.MIL or by mail to the Relief of Liability Section, Disbursing/Debt Management Policy Division, Defense Finance and Accounting Service Indianapolis (DFAS-NPD/IN), Column 329F, 8899 E. 56th Street, Indianapolis, IN 46249. When the Commander is in command of the deputy, agent, or cashier, a copy of the report shall be provided to the DO. The report shall include:

1. The specific type of loss; i.e., physical loss or any payment due to fraud.
2. All known circumstances.
3. If the loss occurred in the imprest fund, then include the authorized amount of the imprest fund.
4. The date the irregularity occurred and/or was discovered.
5. The dollar amount of the loss.
6. The identity of the accountable individual(s) by name, rank/grade, social security number (SSN), and accountable position.
7. The date that an investigation has been or shall be convened.
8. The contact information of the investigative officer (IO); i.e., name, email address, and phone number.
9. The estimated completion date of the investigation, if applicable.
10. The status of any recovery action in progress or contemplated.

060104. Accounting for Losses of Funds

A. General. Specific instructions for recording and clearing losses on the Statement of Accountability ([Standard Form \(SF\) 1219](#)) are stated in [Chapter 19](#) of this volume.

B. Recording a Physical Loss of Funds

1. All physical losses (whether major or minor) are recorded on the DD Form 2657 by increasing line 7.3 (or 9.3, if predecessor DO), "Loss of Funds," and decreasing the appropriate cash on hand line. For example, if a cash count reveals U.S. currency

on hand is short \$100, then decrease line 6.2A and increase line 7.3 or 9.3. Continue to show all losses on the DD Form 2657 and the SF 1219 until recovery or recoupment is made or until relief of liability is granted for the loss.

2. Subsidiary Accountability Record (DD Form 2667) as a Cumulative Record of Physical Losses

a. Support the entry on the DD Form 2657 by recording the loss on the DD Form 2667. Record all physical losses discovered in the DO's account to include those incurred by deputies, agents, cashiers, imprest fund cashiers, and change fund custodians. If more than one physical loss occurs during a single business day, then each loss shall be accounted for individually.

b. Maintain separate DD Forms 2667 by DO for physical losses recorded on lines 7.3 and 9.3.

c. Balance and reconcile to the DD Form 2657 daily.

d. Keep the DD Form 2667 on file as a subsidiary record supporting the DD Form 2657.

e. Complete the DD Form 2667 as follows (See Figure 6-1 for an example of a DD Form 2667 prepared as a cumulative record of physical losses):

(1) Item 1: DSSN. Enter the Disbursing Station Symbol Number (DSSN).

(2) Item 2: Purpose of Record. Enter "Cumulative Physical Losses of Funds."

(3) Item 3: Name of Disbursing Officer. Enter the DO's name and rank/grade.

(4) Item 4: Address. Enter the DO's organization and address.

(5) Item 5: Date. For each loss of funds, enter the date the loss was recorded in the DO's accountability.

(6) Item 6: Reference or Explanation. For each loss, enter a brief description of the loss, including identification of the person responsible for the loss.

(7) Item 7: Increase. For each loss, enter the amount of the loss.

(8) Item 8: Decrease. If relief is granted or recovery/recoupment is obtained, then record the amount accordingly.

(9) Item 9: Balance. Enter the cumulative total of the losses. This balance must be in agreement with the DD Form 2657, lines 7.3 or 9.3 at all times.

f. Forward the DD Form 2667 to DFAS-NPD/IN within 5 calendar days after the end of each month. Forward the DD Form 2667 either by email to disbursing-debtmanagementpolicy@dfas.mil; or fax to dsn 699-0820 or commercial (317) 510-0820; or mail to DFAS-NPD/IN.

3. Agent Losses. Physical losses of funds incurred by deputies, disbursing agents, cashiers, paying agents, collection agents, imprest fund cashiers, or change fund custodians are identified as physical losses within the individual agent's accountability documents. The acknowledgement of the loss shall be made to the DO. The DO then shall reduce the DD Form 2657, line 6.5, for that particular agent and increase line 7.3. The DO shall record the loss on the cumulative DD Form 2667.

4. Change Fund or Imprest Fund Loss. Table 6-3 provides guidance for processing a loss which occurs in a change fund or imprest fund.

5. Counterfeit Currency Loss. The DO shall record the amount of the loss on the DD Forms 2667 and 2657, line 6.2A, "U.S. Currency/Coinage on Hand" (or 6.2B, "Foreign Currency/Coinage on Hand"), column d, by the amount of the counterfeit currency and increase line 7.3.

060105. Investigating Physical Losses of Funds. All physical losses of funds must be investigated. The type of loss determines the type of investigation required.

A Purpose of Investigation. The purpose of the investigation is to review and document all facts leading up to and connected with the loss, to include the:

1. Amount, date, time, and place of the loss;
2. Identification of accountable individuals and others involved;
3. Authenticity of documentary evidence and oral testimony;
4. Functional capacity of the accountable individual incurring the loss and the physical location of this individual (e.g., disbursing office, functional area);
5. Cause of the loss; and,
6. Adequacy of internal controls and whether they were effectively implemented.

Table 6-4 provides questions to use as part of an investigation and to ensure that all facts of the

loss are addressed in order for the investigation to be complete.

B. Minor Physical Losses

1. \$300 or Less (No Fraud). For minor physical losses of \$300 or less, the DO or deputy DO (if the DO is not collocated with the deputy DO) shall conduct the investigation and complete the written investigatory report (See Figure 6-2). If the loss is attributable to the DO, then the investigation shall be conducted, and the written investigatory report prepared by the primary deputy DO. Under no circumstances shall the individual incurring the loss prepare his or her own written investigatory report. In all cases within 30 days from discovery of the loss, the written investigatory report shall be completed and submitted to DFAS-NPD/IN.

2. Over \$300 (No Fraud). For minor physical losses over \$300, someone other than the DO or disbursing office personnel (e.g., a member of the Cash Verification Team) shall be appointed by the commander to conduct the investigation and complete the written investigatory report (See Figure 6-2). The individual appointed to investigate the loss shall have knowledge of disbursing office operations, especially of the required internal controls, pertinent laws, and applicable directives. In all cases within 30 days from discovery of the loss, the investigatory report shall be completed and submitted to DFAS-NPD/IN thru the commander.

C. Major Physical Losses

1. Authority to Appoint IO

- a. The commander of the DO who incurred the loss.
- b. For DFAS sites, the Director of the DO who incurred the loss.
- c. In instances wherein the accountable individual is not located with the DO, the commander over that individual; e.g., commander of a disbursing agent located in Afghanistan would appoint an IO when the agent incurs a loss and the DO is located in Indianapolis.
- d. In those instances where the commander is not authorized to convene an investigation, the commander shall request an investigation through the chain of command.

2. Appointment/Order of IO

- a. Include name of the individual, telephone number, and email address.
- b. Provide matter to be investigated.

c. Cite this volume and any authorizing DoD Component regulation as the authority for the investigation.

d. Specify the approximate period of time allowed for the investigation. NOTE: Investigation is to be completed and forwarded to DFAS-NPD/IN within 90 days from discovery of the loss.

e. Include a copy of the appointment/order in the report of investigation (ROI) as an exhibit.

f. Provide a copy of the official appointment notification within 5 days of appointment to DFAS-NPD/IN.

3. Individuals Authorized to be IOs. Commissioned officer (O-4 or above) or a civilian employee who is senior in rank/grade to person(s) under investigation and:

a. Do not have vested interest in the outcome of the investigation.

b. Are not in the chain of command of the DO or accountable individuals involved in the irregularity.

c. Are familiar with investigative techniques.

d. Have knowledge of financial accounting controls and pertinent laws and directives. (Comptroller personnel shall be used only when there is no feasible alternative to appoint an IO from another organizational element.)

NOTE: Investigative officers without existing extensive backgrounds in investigative or financial matters shall be given technical guidance by the comptroller, staff judge advocate, or DFAS Office of General Counsel (DFAS-DGC).

4. Guidance for IOs

a. Develop all factual information in connection with the loss so that proper action may be taken by higher authority. This shall include information regarding the procedures followed by all individuals involved in the loss, as well as safeguards and controls instituted for the entire period in which the loss occurred.

b. Ensure that each accountable individual receives and reviews this chapter and Chapter 33 of this volume regarding liabilities and responsibilities of accountable individuals and statutory authority (Title 31, United States Code (U.S.C.), sections 3527 and 3528) for relief of liability before interviewing individual(s) for the first time.

c. Obtain evidence concerning the loss in the form of statements from accountable individuals and others involved with the loss. Testimony may be

reported verbatim or summarized by the IO. Whenever possible, the transcript or summary of testimony shall be reviewed, sworn to, and signed by the witness. (When sworn testimony cannot be obtained, the IO shall submit a statement giving the substance of the interview and the reason for absence of attestation.)

d. Allow accountable individual(s) to examine records or documents in the IO's custody that relate to the loss.

e. Gather all records, documents, correspondence, photographs, and sworn affidavits relating to the loss. The IO may use evidence developed in investigations already conducted concerning the loss by other agencies (e.g., Federal Bureau of Investigation (FBI), U.S. Secret Service, or local authorities).

f. Make a determined effort to resolve or clarify all apparent discrepancies or contradictions in the evidence.

g. Report every 30 days on the current status of the investigation. This report shall be sent through the commander to DFAS-NPD/IN.

h. When extraordinary circumstances require an extension to complete the ROI, the IO may request an extension from the commander. Figure 6-3 can be used as a request for an extension. The commander must notify DFAS-NPD/IN of any authorized extension by forwarding Figure 6-3 or similar request to Disbursing-DebtManagementPolicy@dfas.mil.

5. Preparation of the ROI. The ROI shall include the following elements:

a. Facts

(1) Identities of all accountable individuals who are pecuniarily liable for the loss, their SSNs, the amount for which each is accountable, and the involvement of each in the loss.

(2) If any of the individuals involved in the loss are not physically located in the disbursing office, then describe the structure of the chain of command of the activity in which the individual was performing his or her disbursing functions. In addition, describe the financial services supplied by that individual for the activity they serve.

(3) Circumstances leading to, and surrounding, the loss and the efforts undertaken to discover the cause of a loss that remains unexplained.

(4) Description of the internal controls prescribed to prevent losses of the type experienced and the steps taken to implement those controls.

(5) Other relevant information that would aid in understanding how the loss occurred and in evaluating whether relief is appropriate for the

accountable individuals involved.

(6) Documentary evidence (e.g., statements, transcripts, correspondence, affidavits, investigative reports of other agencies, records, and photographs) as exhibits to the ROI.

(7) Information regarding collection activity and any possible offset relating to the loss.

b. Findings. The IO shall make the following findings:

(1) There ((was) or (was not)) a loss to the United States in the amount of (include amount of loss).

(2) The loss ((was) or (was not)) the result of fault or negligence on the part of the accountable individual (i.e., DO, deputy, agent, or cashier).

(3) The loss of (include amount of loss) ((was) or (was not)) ((proximately caused by the negligence of) or (the result of (fraud) or (theft) committed by)) (insert name of individual) when the loss occurs in the internal account of a deputy, agent, or cashier, funds of the imprest fund cashier, custodian of change fund, or other individuals who are entrusted with funds.

(4) The accountable individual (i.e., DO, deputy, agent, or cashier) ((was) or (was not)) carrying out official duties when the loss or deficiency occurred.

NOTE: The IO shall make any other findings that are considered necessary and appropriate. It is essential that the findings as indicated in paragraph 060105.C.5.b be supported by documentation and after each finding, reference shall be made by tab or page number to the supporting documentation.

c. Recommendations

(1) Whether the accountable individual (should) or (should not) be relieved of pecuniary liability for the loss. Separate recommendations concerning each accountable individual involved are required.

(2) Whether any other person or persons (should) or (should not) be held pecuniarily liable for the loss, in whole or in part.

(3) Corrective action for improving controls or procedures, if applicable.

(4) Any other recommendations that are appropriate considering the existing facts, circumstances, and conditions of the case.

6. Submission of ROI

a. Within 90 days after the loss is discovered (unless an extension has been authorized), the IO must submit the ROI through the Commander (who appointed the IO) to DFAS-NPD/IN.

b. Commander's Actions

(1) Immediately review the ROI for compliance with requirements as indicated in paragraph 060105.C5.

(a) Consider all the facts, findings, and recommendations.

(b) Make additional findings and recommendations pertinent to the investigation.

(c) While considering the facts, circumstances, and conditions of the individual case, determine whether sufficient evidence exists to support a recommendation for relief from liability of each accountable individual involved as a part of the ROI.

(d) If sufficient evidence exists, then recommend relief from liability for each accountable individual involved; otherwise, recommend denial of relief setting forth all evidence supporting this denial recommendation. A specific, separate recommendation is required for each accountable individual involved.

(e) If there is evidence of fraudulent or wrongful conduct and the matter is under investigation by the military police, the DoD Component investigative service, and/or the FBI, then those investigative entities may request the report be held until completion of their investigation. If so, then continue to follow-up on the status of their investigation and advise DFAS-NPD/IN every 30 days of the status. Copies of the investigative reports may be added as exhibits before forwarding the report through the chain of command to DFAS-NPD/IN.

(f) Ensure the ROI and all attachments are forwarded to DFAS-NPD/IN within 90 days from discovery of the loss unless the investigation is on hold as indicated in subparagraph (e).

(g) Provide a copy of the ROI to the Commander of the base, station, activity, ship or unit where the accountable individual is located. For Army finance battalions, a copy also shall be transmitted to the parent finance group or finance command. The ROI may be used for disciplinary or administrative action considered necessary by the commander.

(h) Provide to DFAS-NPD/IN any information

that becomes available after the ROI has been forwarded.

(i) Keep one copy of the ROI.

(j) If report is returned by DFAS-NPD/IN because of lack of sufficient information, then ensure that the sufficient information is obtained and returned to DFAS-NPD/IN.

(2) If not complete, then return to the IO explaining the defects and directing supplementation. Notify DFAS-NPD/IN if the ROI cannot be completed and submitted within 90 days from discovery of the loss.

7. DFAS-NPD/IN Action on ROI

a. Review the ROI.

b. When the ROI lacks sufficient information (or in the absence of compliance with the provisions for the findings and recommendations), DFAS-NPD/IN may return the report for further investigation and fulfillment of the provisions as indicated in paragraph 060105.C.5.

c. When the ROI is sufficient, make a recommendation as to liability.

d. Obtain legal review from DFAS-DGC.

e. Forward the recommendation and ROI to the Director, Policy and Performance Management (DFAS-NP). The Director, DFAS-NP, is the ultimate fact finder and makes the final decision on liability for each case.

f. Advise the appropriate individuals of the decision and in those cases wherein individual(s) are held liable, of their right to submit a rebuttal.

060106. Request for Relief

A. Requests for relief shall be in the form of a memorandum and submitted within 30 days after the investigation is completed. A copy of the IO's report shall be included as an attachment to the request for relief. Requests for relief shall be submitted as follows:

1. DOs. Submit request for relief through the Commander or DFAS site director to DFAS-NPD/IN.

2. DOs Settling Accounts of Former DOs. Submit request for relief on behalf of a former DO to DFAS-NPD/IN.

3. Deputy DOs, Disbursing Agents, Cashiers. Submit requests for

relief through the DO responsible for the account to DFAS-NPD/IN.

B. Evidence Required for Granting Relief. An accountable individual entrusted with public monies is held strictly liable for any physical loss of funds placed in the official's care subject to relief of liability as provided by statute. Accordingly, if the Government can establish that a loss has occurred, then strict liability applies to the accountable individual involved with the loss. The accountable individual has the burden of proof and shall be granted relief when the individual presents sufficient evidence that it is more likely than not that the individual:

1. Was not negligent, or
2. The loss was not proximately caused by the individual's fault or negligence.

C. Information Required. When not supplied in the findings of any court of inquiry, investigation, court-martial, or other proceedings (including endorsements thereto), the following information shall be supplied and considered in the request for relief and/or the forwarding endorsements, as appropriate. Failure to include all the information required could contribute to an unfavorable consideration of a request for relief.

1. The specific duty assignment of the accountable individual when the loss occurred.
2. A statement showing when, how, and by whom the loss was discovered.
3. A description of the actions taken to verify the loss and establish how the loss occurred.
4. A statement of when the last cash count and balancing was completed prior to discovery of the loss.
5. A copy of the appropriate standard operating procedures (SOPs) in effect at the time the loss occurred (if no written procedures are available, then a statement shall be prepared setting forth the known and utilized procedures at the time the loss occurred).
6. A statement indicating whether pertinent regulations and instructions were followed or, if not followed, then an explanation and justification for any omissions and deviations.
7. A statement of past involvement, if any, by the individual requesting relief in any prior losses.
8. A statement indicating whether the loss was the result of theft or other criminal act.

9. A description of the manner in which the loss is being carried in the DO's account and the identity of the DO.

D. Forwarding Endorsements. Each addressee in the requestor's chain of command (including the DO) shall provide a forwarding endorsement that shall include a specific opinion as to whether the loss occurred while the accountable individual was in the line of duty and regarding fault or negligence. A specific recommendation as to whether relief should be granted or denied also shall be included as a part of the forwarding endorsement.

060107. Statutory Standards for Relief of a Physical Loss. The general authority to relieve accountable individuals and agents from liability is stipulated in 31 U.S.C. 3527. The relevant provisions are:

A. The Secretary of Defense determines that the official was carrying out official duties when the loss occurred;

B. The loss or deficiency was not the result of an illegal or incorrect payment;
and

C. The loss or deficiency was not the result of fault or negligence by the official.

060108. Funding for Removal of Physical Losses. In all cases, the ideal method for resolving a loss is recovery from the beneficiary of the loss (e.g., recovery of missing cash from the finder or, in cases where the accountable individual(s) is denied relief of liability, collection from the accountable individual(s)).

A. When losses cannot be recovered (including those instances where relief of liability has been denied and recoupment cannot be made from the accountable individual) or relief of liability is granted to the accountable individual, appropriated funds shall be made available to remove the deficiency from the DO's SF 1219.

1. DFAS Employee. If the accountable individual (the individual responsible for the loss of funds) was a DFAS employee or a military member assigned to DFAS when the loss occurred, then DFAS shall identify the appropriation and funding necessary to resolve the loss.

2. Other DoD Component Employees. If the accountable individual was a member or employee of another DoD Component when the loss occurred, then that DoD Component shall identify the appropriation and funding necessary to resolve the loss.

B. The DO shall clear the loss of funds from the DD Forms 2667 and 2657, line 7.3 or 9.3, based on the instructions given by DFAS-NPD/IN.

0602 ERRONEOUS PAYMENTS (ILLEGAL, INCORRECT, AND IMPROPER PAYMENTS)

060201. Definition

A. Any payment that should not have been made or that is an incorrect overpayment under statutory, contractual, administrative, or other legally applicable requirement; and

B. Any payment to an ineligible recipient, any payment for an ineligible service, any duplicate payment, payments for services not received, and any payment that does not account for credit for applicable discounts.

NOTE: This definition applies to accountable individual liability. Improper payments under the Improper Payments Information Act differ, in that, they include both underpayments and overpayments. See Volume 4, Chapter 14 of this Regulation.

060202. Examples of erroneous payments which do and do not require an investigation are included in Table 6-5.

060203 Discovery of Erroneous Payments. See Table 6-6 for processing an erroneous payment.

A. Fraudulent or Suspected Fraudulent Erroneous Payments. The accountable individual or any individual who suspects a fraudulent erroneous payment was made must notify the commander within 24 hours of discovery.

1. Commander's Responsibilities

a. Within 24 hours of notification, report through the chain of command to the Relief of Liability Section, Disbursing/Debt Management Policy Division, DFAS-NPD/IN, per paragraph 060103.C of this chapter.

b. Appoint an IO to conduct a formal investigation. See subparagraph 060105.C of this chapter.

c. Ensure the investigation is completed and forwarded to DFAS-NPD/IN within 90 days of discovery of the erroneous payment.

2. DO's Responsibilities

a. If the erroneous payment occurred due to fraudulent actions of accountable individuals under the direct cognizance or control of the DO, then prepare a collection voucher transferring the amount of the fraudulent payment back into the appropriation from which the payment was disbursed. Increase lines 4.1B "Loss-Refunds", 7.3 "Loss of Funds", or for predecessor losses, line 9.3 "Other" on the DD Form 2657. Report the entry on the DD Form 2667 as prescribed in paragraph 060104.B2 of this chapter.

b. If the erroneous payment occurred due to fraudulent actions by individuals not under the direct cognizance or control of the DO, then the payment(s) shall remain charged to the appropriation originally charged.

B. Erroneous Payments – No Fraud

1. Certifying Officer Responsibilities

a. Review the suspected erroneous payment voucher and the supporting documentation.

b. Ensure collection action is taken against the recipient of the payment as prescribed in Chapter 28 of this volume. This may require submission of the debt to the DO or other responsible area.

c. Notify the commander if the recipient of the erroneous payment does not voluntarily pay the amount owed, and

(1) The debt is delinquent for 90 days, or

(2) The loss cannot be fully recovered within the 2-year period from the time the erroneous payment was made.

2. DO's Responsibilities

a. If the erroneous payment was properly certified, then there are no actions by the DO.

b. If the erroneous payment was not properly certified

(1) Report the loss to the commander.

(2) Ensure collection action is taken against the recipient of the payment as prescribed in Chapter 28 of this volume. This may require submission of the debt to another responsible area. If the erroneous payment is recouped from the recipient, then collect the proceeds into the appropriation which was originally charged unless the appropriation is canceled. If the appropriation is canceled, then refer to Volume 4, Chapter 3 of this Regulation, for disposition of the collection.

3. Commander's Responsibilities

a. Determine the type of investigation to be conducted; i.e., formal or informal.

b. Appoint an IO to conduct the appropriate investigation.

c. Ensure the investigation is completed and forwarded to DFAS-NPD/IN within the established timelines for a formal or informal investigation.

060204. Investigation of Erroneous Payments

A. Formal Investigation Required

1. When fraud (on the part of the payee, disbursing office personnel, certifying officer, or any other accountable individual) is suspected in connection with the payment.

2. When commander determines necessary.

3. Subparagraph 060105.C of this chapter provides guidance relating to formal investigations.

4. The investigation shall be submitted to DFAS-NPD/IN through the Commander who appointed the IO within 90 days from discovery of the erroneous payment.

B. No Formal Investigation Required

1. IO shall prepare investigatory comments using Figure 6-4 as an example.

2. Investigation must be submitted to DFAS-NPD/IN within 60 days from the commander's notification of the erroneous payment.

060205. Statutory Requirements to Relieve Accountable Individuals Pursuant to 31 U.S.C. 3527 and 3528

A. Disbursing Official

1. The payment was not the result of bad faith or lack of reasonable care, and

2. Diligent collection efforts by the disbursing officials and the agency were made.

B. Certifying Officer

1. The certification was based on official records and the certifying officer did not know, and by reasonable diligence and inquiry could not have discovered, the correct information, or

2. The obligation was incurred in good faith, no law specifically prohibited the payment, and the U.S. Government received value for the payment, and diligent

collection efforts were made to recover the payment.

060206. Completion of Loss of Funds Process. When feasible, all actions required to reach a determination of liability for a loss of funds due to an erroneous payment should be completed within 3 years after the date the SF 1219 is certified.

060207. Settlement of Erroneous Payments. As a general rule, losses due to erroneous payments are not carried on the DO's SF 1219 as a loss of funds since an appropriation was charged when the payment in question was made. There are, however, exceptions to this general rule. For example, an exception occurs when the Department of the Treasury issues check issue overdrafts against a DSSN or the payments were made fraudulently by accountable individuals under the direct cognizance or control of the DO.

A. If the erroneous payment is recovered from the recipient, then the appropriation initially charged is credited the amount recouped or collected unless the appropriation is canceled. If the appropriation is canceled, then refer to Volume 4, Chapter 3 of this Regulation, for disposition of the collection.

B. If the erroneous payment cannot be recovered from the recipient and relief of liability has been denied, then the loss shall be collected from the DO, certifying officer, and/or accountable individual(s) involved and the proceeds credited to the appropriation originally charged for the payment unless the appropriation is canceled. If the appropriation is canceled, then refer to Volume 4, Chapter 3 of this Regulation, for disposition of the collection.

C. The amount of the erroneous payment shall remain charged to the appropriation charged when the payment was made when:

1. Relief of liability is granted, and
2. The loss cannot be recovered from the recipient.

If an adjustment to the appropriation account to which the payment was charged is determined necessary, then the amount of the erroneous payment shall be charged as stated in subsection (d)(1) of 31 U.S.C. 3527.

060208. Document Retention. The following documents and information must be retained to properly respond to any audit that may be conducted by the Government Accountability Office (GAO).

A. Detailed statement of facts of the case, including the type of irregularity, date, amount, and names and positions of the accountable individual(s) involved.

B. Reference to pertinent supporting documents, such as pay records, contracts, and vouchers.

C. Description of how the irregularity occurred and how it affected the

accountable individual's account.

D. Adequate description of procedural deficiencies, if known, that caused the irregularity and the corrective action taken or to be taken.

E. Information on any recoupment already made or being considered.

0603 DECISIONS ON LIABILITY. The determination of the Secretary of Defense that relief should be granted is binding. The Secretary of Defense has delegated authority to the Director of DFAS or designee, to make the required determinations and grant or deny relief on all requests for relief of liability. The Director of DFAS has delegated this authority to the Director, DFAS-NP.

060301. Relief Granted. If relief is granted, then DFAS-NP will provide a memorandum with instructions to remove the deficiency or authority to leave the payment charged to the original appropriation.

060302. Relief Denied. If relief is denied, then DFAS-NP will advise the accountable individual(s) of the decision and of their right to submit a rebuttal. The rebuttal must be submitted within 30 days from the date of notification of the adverse determination to DFAS-NPD/IN. Based on the additional information received, DFAS-NPD/IN shall make a recommendation to the Director, DFAS-NP, through the DFAS-DGC, whether to affirm or reverse the previous decision. If the decision is reversed, then the accountable individual(s) will be advised accordingly and the DO will be provided instructions for removal of the loss of funds or authority to leave the payment charged to the original appropriation. If the decision is not reversed, then the commander and/or DO will be advised to take immediate collection action against the accountable individual(s). Procedures for effecting collection of irregularities are prescribed in Chapter 28 of this volume.

0604 OVERAGES OF PUBLIC FUNDS

060401. Overview. Overages are funds held in an amount greater than the amount shown to be on hand by the daily accountability records of the DO.

060402. Recording Overages of Funds. Unless they obviously relate (and the relationship can be documented), do not offset an overage of funds against a physical loss of funds. For example, an obvious relationship usually can be determined if foreign currency on hand is short and U.S. currency on hand is over by equal U.S.-equivalent amounts (for example, an overage of \$431.18 against a loss of \$431.18 foreign currency). Do not offset apparently related overages against shortages if the shortage and overage occur on different business days. Generally, an overage of funds shall be collected into the Budget Clearing Account **F3875 pending a determination of where the overage properly belongs. Subsequently, if no proper location for the overage is determined, the overage shall be transferred from **F3875 to the Department of the Treasury's receipt account, Forfeiture of Unclaimed Money and Property, **R1060. Track overages by recording each occurrence on a separate DD Form 2667 maintained specifically for overages. NOTE: Unlike the cumulative DD Form 2667 maintained

per paragraph 060104.B.2 of this chapter to support specific lines on the DD Form 2657 and the SF 1219, the DD Form 2667 for overages is a stand-alone document for tracking overages. Start a new DD Form 2667 for overages at the beginning of each quarter.

060403. Preparation of DD Form 2667 as a Record of Overages of Funds. List each overage occurring during each day on the DD Form 2667. See Figure 6-5 of this chapter for an example of DD Form 2667 prepared as a record of overages. Complete the form as follows:

- A. Item 1: DSSN. Enter the DSSN.
- B. Item 2: Purpose of Record. Enter “Overage of Funds.”
- C. Item 3: Name of Disbursing Officer. Enter the DO’s name and rank/grade.
- D. Item 4: Address. Enter the DO’s organization and address.
- E. Item 5: Date. For each overage of funds, enter the date the overage was collected into a deposit fund account or miscellaneous receipt account, as appropriate.
- F. Item 6: Reference or Explanation. For each overage, enter a brief description of the overage together with identification of the person responsible for the overage (if known); when disposition is determined, give a brief description.
- G. Item 7: Increase. For each overage, enter the amount of the overage.
- H. Item 8: Decrease. This item is not used on the DD Form 2667 maintained for overages.
- I. Item 9: Balance. Enter the cumulative total of the overages shown in the record.

060404. Reporting Overages of Funds. Overages of funds that are \$750 or more must be reported to the Commander. However, unless there is an indication of fraud or other criminal act, there is no requirement to report or investigate as in losses of funds. A copy of the DD 2667 shall be retained with the original voucher transferring the funds to the **R1060 account.

[illegible]

DD Form 2667, AUG 93

**Figure 6-1. DD Form 2667, “Subsidiary Accountability Record”
(Cumulative Physical Losses of Funds)**

MINOR PHYSICAL LOSSES—NO FRAUD				
1. Loss Amount		2. Date of Loss		3. Date Loss Discovered
4. Location of Loss			5. DSSN	
Accountable Individuals				
6. CAPACITY	7. NAME	8. SSN	9. GRADE	10. MAILING ADDRESS
DO				
DEPUTY				
AGENT				
CASHIER				
OTHER				
11. How did Loss Occur?				
12. Did accountable individuals act in a prudent manner in compliance with regulations, procedures, etc.? Yes No (If no, provide name of individual(s) and reason(s))				
13. Were accountable individuals acting within their line of duty? Yes No (If no, provide name(s) and reason(s))				
14. Has the presumption of the accountable individuals' negligence been refuted? Yes No (If no, provide name(s) and reason(s))				
15. Where the loss was by a subordinate, did the supervisory DOs(s)/deputy DOs exercise adequate supervision? If, YES, identify and attach applicable procedures; e.g., SOPs, training guides, inspection results, etc. If NO, provide reasons.				
16. I do recommend relief of liability _____			17. I do not recommend relief of liability _____	
18. The accountable individuals have been counseled regarding appropriate corrective measures to prevent recurrence and the applicable regulatory procedures for minor losses of funds have been reviewed. Yes _____ No (provide reasons) _____				
19a. _____ does request relief of liability _____. Additional facts provided in separate memo YES___ NO___			19b. _____ does not request relief of liability _____.	
20. POC for this investigation is _(Name (to include grade/rank), (Phone Number), and (EMAIL address))				

Figure 6-2. Minor Physical Losses-No Fraud

BLOCK	GUIDANCE
1	Insert dollar amount of loss.
2	If known, insert date loss occurred. If unknown, leave blank.
3	Insert date loss was discovered.
4	Insert the location wherein the loss occurred; e.g., Incirlik Air Base, Turkey; USS EISENHOWER; Camp Arifjan, Kuwait.
5	Insert the disbursing station symbol number that incurred the loss.
6	Identify each accountable individual, to include the DO, deputy, and the individual that incurred the loss.
7	Include the full name of appropriate individuals.
8	Provide the social security number of each individual.
9	Include the grade/rank of the appropriate individuals; e.g., GS 4 (civilian) or military rank.
10	Provide the mailing address of each individual.
11	Provide details of how the loss occurred; e.g., "Cashier was performing standard disbursing functions; i.e., check cashing, casual pays, etc., in a combat zone. When cashier returned funds/documents to disbursing agent, a \$100 shortage was discovered. Cashier had no explanation for the loss."
12	Respond to this. Note: What "prudent" or "non-negligent" is requires applying the standard of reasonable care or ordinary negligence. Negligence is determined by applying a reasonable prudent person (RPP) test. The test requires the fact finder to weigh the facts of the case against what a reasonable person would have done to take care of his or her own property of like description under similar circumstances. Therefore, a determination of negligence is a highly fact-sensitive inquiry and what constitutes "reasonable" or "prudent" under the RPP test is wholly dependent on the facts, conditions and circumstances presented by each case.
13	Provide Response. Normally the response will be "yes". A "no" response would be rare.
14	The fact that a loss or deficiency occurred gives rise to a presumption of negligence on the part of the accountable individual. An accountable individual bears the burden of producing evidence to rebut this presumption. The presumption may be rebutted by evidence that demonstrates that it is more likely than not that the accountable individual was not negligent. In other words, the greater weight of the evidence, though not sufficient to free the mind wholly from all reasonable doubt, is sufficient to incline a fair and impartial mind that the accountable individual was not negligent relating to the loss. Regarding negligence, see guidance in Block 12.
15	When a DO is liable as the result of a physical loss by a subordinate and not as the result of direct involvement, the DO may be relieved if he/she maintained adequate supervisory control over the operations. If this is the case, list those controls; e.g., Cashier SOP, training guides, etc.
16	If you recommend relief, complete with the names of the accountable individuals.
17	If relief is not recommended, complete with the names of the accountable individuals.
18	Indicate if the appropriate individuals have been counseled and applicable regulatory procedures have been reviewed. If not, provide reasons; e.g., individual discharged.
19a	Insert the name of the individual(s) requesting relief. If the individual(s) requests relief and has additional information not included in the investigation, a separate memo must be provided to DFAS-NPD/IN within 30 days after completion of the investigation.
19b	Insert the name of the individual who does not request relief. If the individual chooses not to request relief, he/she must pay the amount of the loss.
20.	Provide the IO's name to include grade/rank, phone number, and email address.

Figure 6-2. Minor Physical Losses—No Fraud (Continued)

REQUEST FOR EXTENSION OF INVESTIGATION
COMPLETION BY INVESTIGATIVE OFFICER
1. FROM:
2. TO:
3. REQUEST EXTENSION TO COMPLETE INVESTIGATION OF \$ _____ LOSS OF FUNDS
4. DATE REQUESTED FOR EXTENSION:
5. REASON FOR REQUEST:
COMPLETION BY COMMANDER WHO APPOINTED INVESTIGATIVE OFFICER
6. COMMANDER APPROVED: _____
7. COMMANDER DISAPPROVED/REASON:

Figure 6-3. Request for Extension of Investigation

ERRONEOUS PAYMENTS-NO FRAUD					
1. Loss Amount		2. Appropriation		3. Date of Loss	
4. Date Loss Discovered		5. Location of Loss		6. DSSN	
7. DISBURSING OFFICER/DEPUTY DISBURSING OFFICER					
7a. NAME		7b. SSN	7c. GRADE/RANK		7d. MAILING ADDRESS
7e. Was payment made based on properly certified voucher?			Yes	No, provide reason	
7f. Was payment the result of bad faith or lack of reasonable care on part of the DO?		Yes, provide reason			No
7g. If required, did DO take diligent collection actions?		Yes, provide synopsis of actions taken.		No, provide reasons	
8. CERTIFYING OFFICER					
8a. NAME		8b. SSN	8c. GRADE/RANK		8d. MAILING ADDRESS
8e. Was certification based on official records and the official did not know and by reasonable diligence and inquiry could not have discovered the correct information?					
8f(1) Was obligation incurred in good faith?					
8f(2) Did a law specifically prohibit the payment?			8f(3) Did U.S. Government receive value for the payment?		
8g. If required, did certifying officer take diligent collection actions?			Yes, provide synopsis of actions taken		No, provide reasons
9. INVESTIGATING OFFICER					
9a. NAME		9b. SSN	9c. GRADE/RANK		9d. MAILING ADDRESS
10. I do recommend relief of liability _____			11. I do not recommend relief of liability _____ (Provide reasons)		
12a. The individual does request relief of liability _____.					
12b. The individual does not request relief of liability _____.					

Figure 6.4. Erroneous Payments – No Fraud

BLOCK	GUIDANCE
1	Insert dollar amount of loss.
2	Provide the appropriation in which the payment was charged.
3	Insert date loss occurred.
4	Insert date loss was discovered.
5	Insert the location wherein the loss occurred; e.g., Incirlik Air Base, Turkey; USS EISENHOWER; Camp Arifjan, Kuwait.
6	Insert the disbursing station symbol number that incurred the loss.
7a, b, c, d	Identify the DO/deputy DO who made the payment by providing his/her name, social security number, grade/rank of individual(s), and a mailing address.
7e	If the payment was made on a properly certified voucher by a duly appointed certifying officer, check “Yes”. If not, provide the reason(s), it was not.
7f	“Bad faith” can be considered somewhere between negligence and dishonesty, and closer to the latter. Whether the DO exercised reasonable care is determined by applying a reasonable prudent person (“RPP”) test. The test requires the fact finder to weigh the facts of the case against what a reasonable person would have done under similar circumstances. Therefore, a determination of reasonable care or negligence is a highly fact sensitive inquiry and what constitutes “reasonable” under the RPP test is wholly dependent on the facts, conditions and circumstances of each case.
7g	If required and the DO took diligent collection action in accordance with the DoDFMR, Volume 5, Chapter 28, please answer “yes” and provide a synopsis of what actions were taken.
8a, b, c, d	Identify the certifying officer who certified the accuracy of facts stated on the voucher, computation of the certified voucher, and legality of the payment by providing his/her name, social security number, grade/rank of individual(s), and a mailing address.
8e	Provide an explanation of what documentation the certifying officer used to certify the payment. If the certification was based on incorrect facts, could the certifying officer have determined the true facts?
8f(1)	Did the certifying officer have, or should have had, doubt regarding the propriety of the payment, and if so, what he or she did about it.
8f(2)	Is there a statute that prohibits the payment? If yes, please provide.
8f(3)	Value received normally implies receipt of goods or services with a readily determinable dollar value; however, an intangible item may constitute value received where the payment has achieved a desired program result.
8g	If required and the certifying officer took diligent collection action in accordance with the DoDFMR, Volume 5, Chapter 28, please answer “yes” and provide a synopsis of what actions were taken.
9a, b, c, d	Investigative Officer must include this information. This will provide DFAS-NP with a point of contact, if needed.
10	If relief is recommended, please complete.
11	If the recommendation is to deny relief, please provide reasons.
12a	If the individual requests relief and has additional information not included in the investigation, a separate memo must be provided to DFAS-NPD/IN within 30 days after completion of the investigation.
12b	If the individual chooses not to request relief and the debt is uncollectible from the recipient of the payment, he/she must pay the amount of the loss.

Figure 6-4. Erroneous Payments—No Fraud (Continued)

[illegible]

DD Form 2667, AUG 93

Figure 6-5. DD Form 2667, Subsidiary Accountability Record (Overage of Funds Record)

PHYSICAL LOSS EXAMPLES	
TYPES OF LOSSES	EXPLANATION
Public Funds	Loss of cash.
Limited Depository Account (LDA)	A loss can occur when LDA account is unreconciled, incorrectly reported, or has been subject to a fraudulent transaction.
Records	Loss of debit vouchers, deposit tickets, etc.
Original Vouchers	NOTE: If the original voucher is lost and the DO's retained copy (and the retained supporting documents) is available, then the copy may be stamped as a certified copy of the original voucher. However, the absence of a signature acknowledging receipt of a cash payment may negate the validity of the certified copy. The same is true when a payee denied receipt of a cash payment and there is no original voucher (with the payee's signature) to provide proof payment was made.
Documentation Supporting Debit Vouchers	A physical loss can occur if open debit items cannot be cleared because of the loss of supporting documentation.
Shipment of Cash	Shipment of cash which becomes lost can result in the liability of the accountable individual(s) when they failed to ship cash as required by <u>Chapter 3</u> of this volume, and the loss is not covered under the Government Losses in Shipment Act.
Unexplained Losses	No explanation – money is missing.
Negotiable Instruments	A physical loss can result when a negotiable instrument and all copies held in the disbursing office are lost.
Bank Failure	DO's funds in a bank; e.g., a limited depository account and the bank closes because of failure.
Counterfeit Currency	Currency in the DO's possession which is determined to be counterfeit.
Change Fund	Cash shortage that cannot be made whole from sales receipts.
Imprest Fund	Shortage of funds advanced to imprest fund cashier.
Fraud within Disbursing	A loss resulting from fraudulent actions of disbursing personnel acting alone or in collusion with others.
Robbery, burglary	A loss of funds resulting when a robbery/burglary transpires.

Table 6-1. Physical Loss of Funds Examples

PROCESSING LOSSES OF FUNDS DUE TO PHYSICAL LOSS

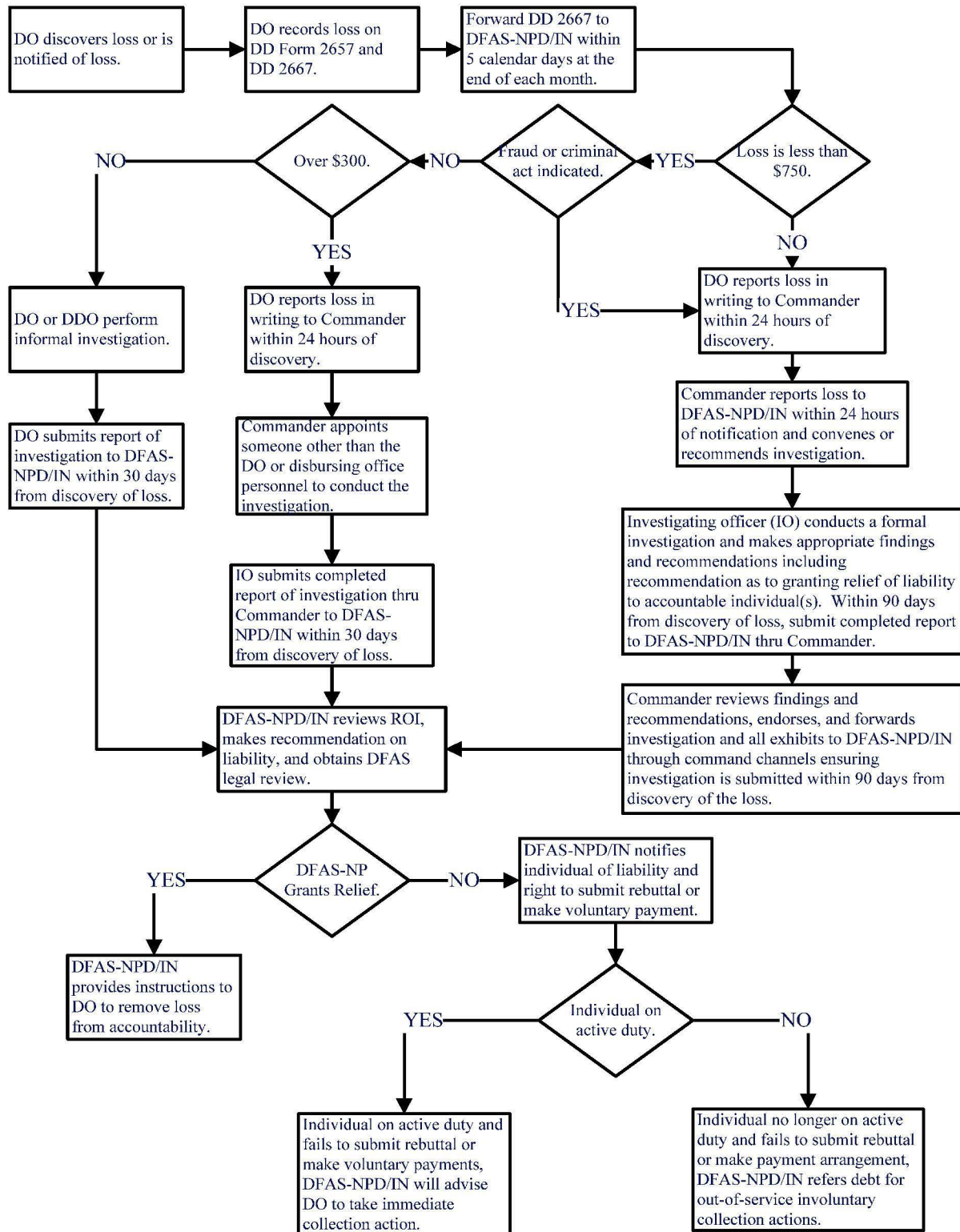


Table 6-2. Processing Physical Losses of Funds

IF		CHANGE FUND CUSTODIAN OR IMPREST FUND CASHIERS SHALL	DO SHALL	COMMANDER SHALL
A cash shortage in the change fund is made whole from sales receipts (property),	Then, there is no loss of funds.			
A cash shortage in a change fund cannot be made whole from sales receipts,	Then, the balance of the shortage is considered a loss from the change fund.	Make a return (on paper only) of the amount of the loss using the Statement of Agent Officer's Account (DD Form 1081).	Upon receipt of DD Form 1081, record the change fund loss on the DD Form 2667 and on the DD Form 2657 as a decrease to line 6.5 and increase to line 7.3.	<p>If loss is a major loss of funds, take actions to report loss and convene or request appropriate investigation as specified in paragraphs 060103.C and 060105.C of this chapter.</p> <p>If loss is a minor loss of funds, ensure investigation is conducted per paragraph 060105.B of this chapter.</p>
A loss of all activity funds (sales receipts and change fund)	Is considered a loss of funds and	Make a return (on paper only) of the amount of the loss using the DD Form 1081.	Upon receipt of DD Form 1081, record the change fund loss on the DD Form 2667 and on the DD Form 2657 as a decrease to line 6.5 and increase to line 7.3.	<ol style="list-style-type: none"> 1. If loss is major loss of funds, report loss as specified in paragraph 060103.C of this chapter. 2. Initiate a report of survey for the loss of sales receipts. The report of survey investigation, plus any other investigations (e.g., FBI) shall cover the facts and circumstances surrounding the entire loss (change fund and sales receipts). The report of survey determines liability only for the loss of sales receipts. Since the same set of facts and circumstances relates to both the losses of sales receipts and change funds, a separate investigation is not required for the loss of change fund. 3. Send a summary report of the investigation to DFAS-NPD/IN. The report shall include: <ol style="list-style-type: none"> a. Certification that the DO (or authorized agent) advanced the change fund per this volume. b. Statement of whether the safeguarding requirements prescribed in this volume were met (and if not met, the reason(s) why). c. Determination that satisfactory evidence exists to support a recommendation for relief of the DO or any other person involved, or a finding of pecuniary liability against the DO or any other person involved. d. Copy of the report of survey (and all attachments).

Table 6-3. Processing Change Fund or Imprest Fund Loss

IF		CHANGE FUND CUSTODIAN OR IMPREST FUND CASHIER SHALL	DO SHALL	COMMANDER SHALL
A loss occurs in an imprest fund,		Upon discovery, report loss to DO or authorized agent who advanced the funds through the commander who approved establishment of funds, and Make a return (on paper only) of the amount of the loss using the DD Form 1081.	Upon receipt of DD Form 1081, record the change fund loss on the DD Form 2667 and on the DD Form 2657 as a decrease to line 6.5 and increase to line 7.3.	1. If loss is a major loss of funds, take actions to report loss and convene or request appropriate investigation as specified in paragraphs 060103.C and 060105.C of this chapter. 2. If loss is a minor loss of funds, ensure investigation is conducted per paragraph 060105.B of this chapter.
		Upon receipt of additional advance, if applicable, provide the DO with a signed DD Form 1081.	If commander determines imprest fund should be restored to its full operational level, make advance following procedures described in Chapter 2 of this volume except the amount of the advance shall not be recorded as an increase to DD Form 2657, line 6.5. Record the loss on the DD Form 2667 and record the additional advance on line 7.3 of the DD Form 2657.	Based on information contained in imprest fund cashier's report and amount of loss, volume of imprest fund transactions, and frequency of replenishment, determine whether DO should provide additional advance in amount of loss to restore imprest fund to its full operational level. If decision is to provide additional advance, notify the DO of requirement in writing. a. Include information as to whether imprest fund will be turned over to alternate cashier pending completion of the required investigation(s) and b. Provide instructions of the additional advance to the primary or alternate cashier, as appropriate.

Table 6-3. Processing Change Fund or Imprest Fund Loss (Continued)

Question	Cashier Loss	Counterfeit Currency Loss	Agent Officer Loss	Fraud Loss	Imprest Fund Cashier and Change Fund Custodian Loss
Have the DO and any other person who might be held liable for the loss been afforded all the rights and privileges of parties in interest?	X	X	X	X	X
Has testimony been obtained from every person who may have relevant information regarding the circumstances?	X	X	X	X	X
Has each witness been thoroughly questioned?	X	X	X	X	X
Are there inconsistencies among the testimonies of different witnesses?	X	X	X		X
Has a thorough investigation been made in order to discover the full extent of the loss?	X	X	X	X	X
Have other investigations of the loss been considered? (NOTE: Do not consider lie detector test results.)	X		X	X	X
If fraud is involved, have the methods used to defraud the U.S. Government been clearly described?				X	
Has the cause of the loss been clearly established?	X	X	X	X	X
Was a thorough search of the physical area made for missing cash or vouchers?	X		X		X
Were the transactions made during the day of the loss thoroughly reviewed in an effort to determine the cause of the shortage?	X		X		X
Were any individuals contacted in an effort to determine if an overpayment had been made and could be recovered?	X		X		X
Were individuals who made collections contacted to determine if they found a compensating overage in their accounts?	X		X		X
Was all the cash-on-hand counted to make sure that there was no compensating overage?	X		X		X
What was the number of transactions handled by the cashier/agent during the period in which the loss occurred?	X		X		X
Did distracting influences exist or were working conditions poor?	X	X	X		X
Was the cashier/agent working under pressure because of the heavy volume of business?	X	X	X		X
Was the cashier/agent handling new currency that has a tendency to stick together?	X		X		X
Was the cashier/agent experienced or inexperienced?	X		X		X
What procedures and internal controls has the DO established for safeguarding funds and to preclude fraudulent activity?	X		X	X	X
What facilities were furnished to protect cash for which the cashier/agent was accountable, such as a cash drawer with key lock or a separate safe?	X		X		X
What procedures were followed by the DO, deputy DO, and/or disbursing agent in making daily settlements with the cashier?	X				
Has the DO supplied instructions in detecting counterfeit money for those personnel in the office that handle money?		X			
What written SOPs has the DO supplied for guidance?	X	X	X		
Are the SOPs adequate?	X		X		
Did the accountable individual follow the applicable procedures on the day of the loss?	X	X	X	X	X

Table 6-4. Questions to Use for Investigations

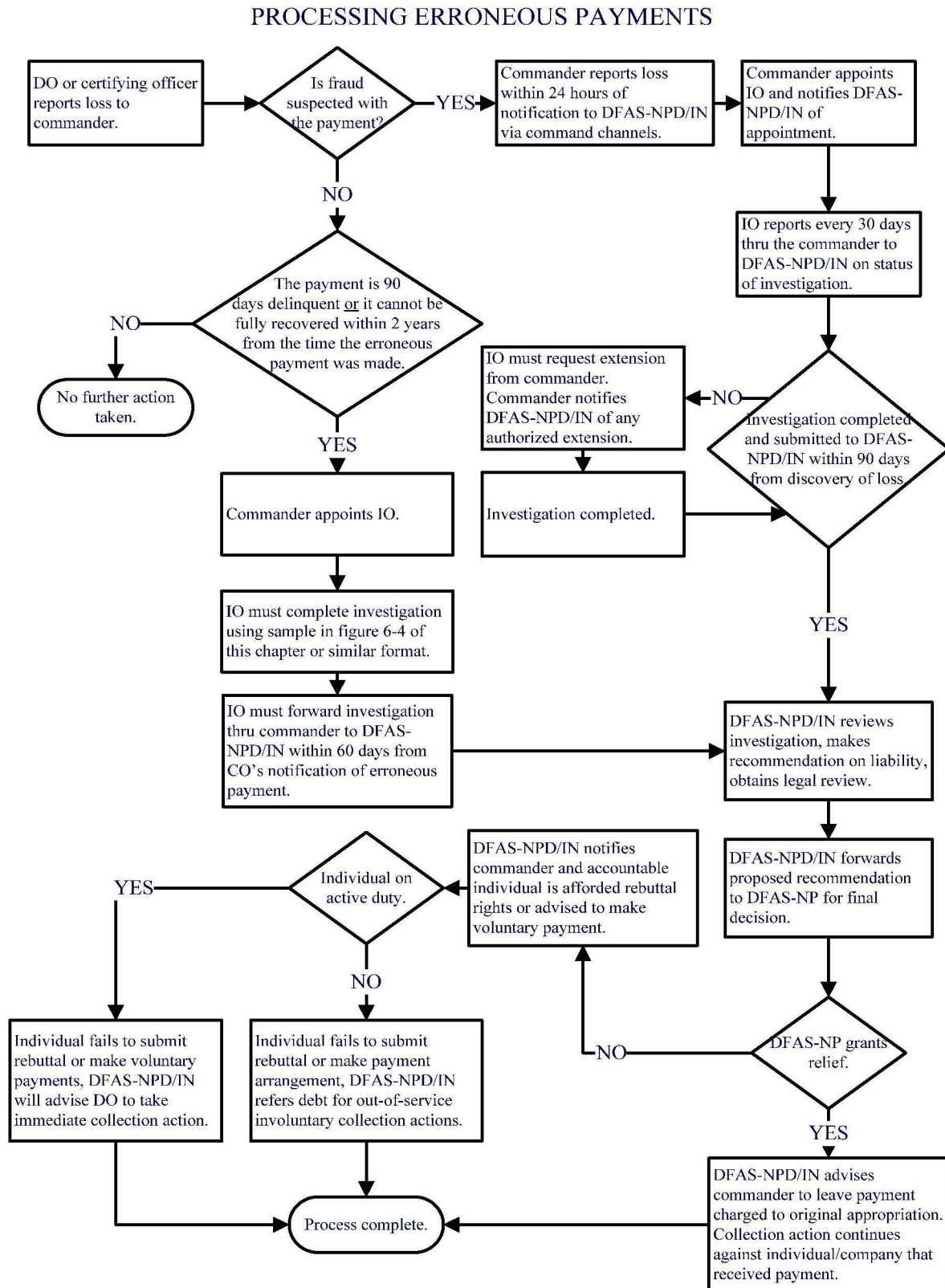
Question	Cashier Loss	Counterfeit Currency Loss	Agent Officer Loss	Fraud Loss	Imprest Fund Cashier and Change Fund Custodian Loss
Has the DO issued any oral instructions?	X	X	X		
Was the cashier's cage or safe accessible to persons other than the cashier/agent?	X		X		
Did theft occur?	X		X		X
Does the exhibit show the appointment of the individual; i.e., cashier, deputy, agent, etc.?	X		X		X
Was the cashier/agent functioning under the direct cognizance/control of the DO?	X		X		
When, and by whom, was the receipt of counterfeit currency detected?		X			
Was an effort made to determine the source of the counterfeit note(s)?		X			
Does the volume of transactions handled by the cashier/agent preclude a careful inspection of each and every piece of currency?		X			
Do exhibits show the amount the DO entrusted to the cashier/agent, the signature of the cashier/agent in receipt of funds, the turn-in made by the cashier/agent, and the amount of the shortage or a statement of the cashier's/agent's account?	X		X		
If the loss involves funds in the hands of a cashier/agent, has the DO inspected and supervised the cashier/agent office, or arranged for such inspections?	X		X		
Under what functional capacity was the accountable individual acting with regards to the DO?				X	
What is the accountable individual's immediate chain of command within the activity for which they provide disbursing services?				X	
Has all possible collection action been taken?				X	
In the case of military personnel, is collection action being taken in the field or by the supporting DFAS site in cases when personnel have been separated from the Service?				X	
In the case of civilian employees, has the individual involved authorized application of pay to offset the shortage? Have steps been taken to secure application of final pay to settle the indebtedness? If the amount of the indebtedness has been determined, has a request been made to Office of Personnel Management for offset against the Civil Service Retirement and Disability Fund?				X X X	

Table 6-4. Questions to Use for Investigations (Continued)

ERRONOUS PAYMENTS WHICH REQUIRE AN INVESTIGATION
1. Any of the following payments in which the debt is delinquent for 90 days or the loss cannot be fully recovered within the 2-year period from the time the erroneous payment was made
2. Overpayment to a payee
3. Payment to the wrong payee
4. U.S. Treasury check issue overdrafts
5. Negotiation of both original and replacement U.S. Treasury checks
6. Any payment based on fraudulent, forged, or altered documents prepared or presented by individuals not under the direct cognizance/control of the DO
7. Payment in violation of a regulation

ERRONEOUS PAYMENTS WHICH DO NOT REQUIRE AN INVESTIGATION
1. An erroneous payment that is not delinquent for 90 days and can be recovered within the 2-year period from the time the erroneous payment was made
2. An erroneous payment which is collectible through offset of military pay, civilian pay, retired pay, contract debt
3. A valid payment made in accordance with appropriate documentation which through no fault of the certifying officer becomes an overpayment; e.g., (1) A member paid a reenlistment bonus and subsequently does not complete terms of contract (2) a deceased retiree who is overpaid because death notification not provided; (3) an overpayment on a travel advance
4. A payment made based on documentation from an individual and certified to be true, correct; e.g., a payment made to the wrong bank account because the individual provided incorrect information
5. Any payments made based on vouchers not examined under an approved statistical sampling plan

**Table 6-5. Examples of Erroneous Payments Requiring an Investigation
and Payments Not Requiring an Investigation**

**Table 6-6. Processing Erroneous Payments**

ATTACHMENT N

MONTHLY SUMMARY REPORT

NAME OF E&E FUND ACCOUNT: _____

MONTH: _____ YEAR: _____

- | | | |
|--|-------|---------|
| 1) TOTAL FUNDS AVAILABLE AT START OF PERIOD: | _____ | (TAB 1) |
| 2) TOTAL FUNDS RECEIVED DURING PERIOD: (+) | _____ | (TAB 2) |
| 3) TOTAL EXPENDITURES DURING PERIOD: (-) | _____ | (TAB 3) |
| 4) TOTAL FUNDS TRANSFERRED DURING PERIOD: (-) | _____ | (TAB 4) |
| 5) TOTAL FUNDS AVAILABLE AT END OF PERIOD: (=) | _____ | (TAB 5) |

Funds available should equal the sum of the following:

Cash on Hand Balance:	_____	
Pending Advances: (+)	_____	(attach list detailing agent name, amount, and date of advance)
Bank Account Balances: (+)	_____	(attach bank account reconciliation worksheet)
Total: (-)	_____	(should equal amount reported in item 5 above)

BANK ACCOUNT INTEREST PAYMENTS :

- Interest cannot be used to supplement appropriated funds and cannot be included in funds available balance
- Interest must be returned to the Treasury on or before September 30 of each year.

- | | | |
|--|-------|---------|
| 1) INTEREST RECEIVED FISCAL YEAR TO DATE AS OF START OF PERIOD: | _____ | |
| 2) INTEREST RECEIVED DURING PERIOD: (+) | _____ | |
| 3) INTEREST PAYMENTS RETURNED TO THE TREASURY DURING PERIOD: (-) | _____ | |
| 4) NET INTEREST REMAINING IN ACCOUNT: (-) | _____ | (TAB 6) |

CUSTODIAN CERTIFICATION:

I certify that the above information was prepared from the attached source documents and that to the best of my knowledge and belief it is complete and accurate. I have reconciled the above referenced account in accordance DCIS SAM Chapter 10 and I have found no loss or discrepancy.

Name of Custodian

Signature and Date

MANAGEMENT APPROVAL:

I have reviewed and approved this report and the claimed expenses in accordance with DCIS SAM Chapter 10.

Name of Approving Official

Signature and Date

Title of Approving Official

Law Enforcement Sensitive (when filled in)
DCIS Form 75A, NOV 2006 (Previous Editions are Obsolete)

ATTACHMENT O

E&E ACCOUNT RECONCILIATION WORKSHEET

NAME OF ACCOUNT: _____
AS OF: _____ (End date of the period covered)

- 1) CASH-ON-HAND: \$0.00 (Funds maintained in cash by custodian)
2) PENDING ADVANCES: \$0.00 (Unexpended balance of funds advanced to agents)

Name of Agent	Date of Advance	Amount
1)		
2)		
3)		
4)		
5)		
6)		
7)		
8)		
9)		

- 3) BANK BALANCE: _____ (Result of calculation below)

STATEMENT BALANCE		
TOTAL OF ALL INTEREST PAID TO DATE		Less
CREDITS NOT POSTED ON STATEMENT		Plus
Date	Amount	
1)		
2)		
3)		
4)		
5)		
6)		
7)		
8)		
9)		

DEBITS NOT POSTED ON STATEMENT			Less
Date	Check No.	Amount	
1)			
2)			
3)			
4)			
5)			
6)			
7)			
8)			
9)			

- 4) PENDING TRANSFERS: _____ (transfers not yet received by another E&E account)
5) PENDING CREDITS: _____ (credits posted to third party accounts, such as credit cards)
6) FUNDS AVAILABLE AT END OF PERIOD: _____ (Sum of 1 through 3 above)

NAME: _____ DATE: _____
(Printed name of person reconciling account)

CHAPTER 12

TECHNICAL SERVICES PROGRAM

<u>Contents</u>	<u>Section</u>
General	12.1.
Definitions	12.2.
Applicability and Scope	12.3.
Policy	12.4.
Staffing and Organization	12.5.
Technical Investigative Equipment (TIE)	12.6.
Technical Training and Safety	12.7.
Requesting Technical Support	12.8.
Technical Support Doctrine	12.9.
Products of Technical Surveillance	12.10.
Documentation of Technical Surveillance	12.11.
Testimony and Press Releases	12.12.

12.1. General. The DCIS Technical Services Program encompasses all electronic surveillance, technical support of investigations, and investigative communications.

12.2. Definitions

12.2.a. **Interception.** The acquisition of the contents of any wire, oral, or electronic communication through the use of any electronic, mechanical, or other device. The term “contents” includes any information concerning the identities of the parties to such communication or the existence, substance, purpose, or meaning of that communication.

12.2.b. **Intercept Equipment.** Technical Investigative Equipment (TIE) that is specifically designed, procured, and operated for the purpose of intercepting wire, oral, or electronic signal communications. The possession and use of these items is restricted by federal and state law and requires special handling, storage, and control. Refer to Special Agents Manual (SAM) Chapter 11, “Interception of Wire, Electronic, and Oral Communications,” for the proper use, storage, control, and disposition of intercept equipment.

12.2.c. **Special Purpose Vehicle (SPV).** An undercover vehicle equipped and used exclusively for conducting technical surveillance.

12.2.d. **Technical Investigative Equipment (TIE).** All hardware used specifically for conducting or supporting technical surveillance investigative operations.

12.2.e. **Technical Services Agent (TSA).** A DCIS special agent (SA) who has successfully completed specialized technical training and possess an extensive work history in a technically related field. The TSA is assigned full-time technical service duties within Headquarters, DCIS Technical Services Program. The lead TSA is the Technical Services Program Manager (TSPM) and oversees all technical services activities.

12.2.f. **Technical Services.** This term encompasses all aspects of technical surveillance, support, and investigative communications including the areas of equipment operation, procurement, maintenance, disposal, inventory, training, forensic processing, and media duplication.

12.2.g. **Technical Support Specialist (TSS).** A DCIS SA who has successfully completed a prescribed course of basic technical training and is assigned the collateral duty of providing limited technical services within the local DCIS Field Offices' (FO) geographically assigned area of responsibility.

12.2.h. **Technical Surveillance.** The collection of evidence through the use of intelligence gathering methods, electronic, mechanical, or other devices.

12.2.i. **Technical Review Allocation Committee (TRAC).** The TRAC committee consists of HQ and field personnel chosen by the Program Director, Special Operations who possess knowledge in the use of TIE and future TIE requirements. The TRAC is responsible for the review and majority vote approval of all TSA proposed procurements. The TRAC may review, vote, and approve additional procurement submissions from the field and within the committee, based on funding availability.

12.3. **Applicability and Scope**

12.3.a. The provisions of this chapter apply to all SAs and support personnel within DCIS and any personnel assigned to DCIS on a temporary basis.

12.3.b. This chapter provides guidance in the management and responsibilities of the DCIS Technical Services Program. It is not intended to supersede SAM Chapter 11, "Interception of Wire, Electronic, and Oral Communications," but to complement it by specifically addressing management and administrative issues that are unique to technical services. Additionally, this chapter is not intended to be a technical guide or manual about the operation or maintenance of specific equipment.

(b)(7)(E)

12.5. Staffing and Organization

12.5.a. Selection of TSS and TSA Personnel. TSS personnel are selected and assigned to technical duties by their respective Special Agent in Charge (SAC). As necessary, a SAC may delegate this authority to subordinate supervisors. TSA personnel are selected and assigned to perform technical duties by the Program Director, Special Operations.

12.5.b. Technical Support Specialist (TSS). A TSS is a DCIS SA who has successfully completed a prescribed course of basic technical training and is assigned the collateral duty of providing limited technical services within the DCIS FOs' geographically assigned area of responsibility. The TSS is assigned to a standard DCIS SA position description.

12.5.b.(1). Selection Guidance. A progressive level of knowledge, training, and experience is needed to properly perform the increasingly complex disciplines of technical surveillance operations. To this end, SAs performing technical service duties receive complex and valuable training and are expected to maintain and continually upgrade their level of technical knowledge. The respective SAC or a designated representative will assign a primary TSS and an alternate TSS per field office. Those assigning persons to technical services duties should carefully consider the continuing availability and retention of those persons. Additionally, the prospective TSS must be favorably evaluated on the following factors: technical aptitude and knowledge, willingness to perform technical service duties, continuing availability (with due respect to the SA's other duties and responsibilities), and the ability to relate technical concepts to others. Generally, SAs below the grade of GS-12 should not be assigned TSS duties. These SAs are still in training for their primary criminal investigator duties and should focus their attention towards that training. When necessary, because of staffing levels, the SAC may waive the grade level requirement.

12.5.b.(2). Duties and Responsibilities. A TSS is responsible for conducting consensual monitoring, photography, and camcorder-based videography. These duties serve as the baseline for TSS performance. It is not required that TSSs perform all technical duties within their field office. When deemed appropriate by the local supervisor, a TSS may train other SAs to perform some basic, recurring, technical tasks. However, DCIS invests valuable resources to train TSSs to perform technical duties. As such, the TSSs are best prepared for and should perform these tasks whenever possible. As mission requirements dictate, TSSs may receive additional training and perform duties in other technical surveillance disciplines. However, TSSs must not perform technical tasks that exceed their level of training and competence.

(b)(7)(E)

(b)(7)(E)

12.5.b.(4). **Supervision.** A local supervisor (for example, Resident Agent in Charge or Group Manager) manages the TSS. Supervisors should carefully weigh the level of effort required to perform technical duties successfully. It is important to note that TSS duties often require extensive time and effort. Hence, when deemed appropriate by the supervisor, the TSSs performance plan and evaluation should accurately reflect these duties and the associated workload. Supervisors are encouraged to include technical duties as critical factors in the TSSs performance plan. The TSS receives technical advice, assistance, and guidance from the TSAs assigned to the DCIS Technical Services Program. Supervisors are encouraged to solicit input from the DCIS TSPM on performance evaluations of TSSs.

12.5.c. **Technical Services Agent (TSA).** TSA is a DCIS SA who has successfully completed extensive technical training and has an extensive work history in the technical field. The TSA is assigned full-time technical service duties.

(b)(7)(E)

12.5.c.(2). **Selection Guidance.** Persons assigned as TSAs perform DCIS's most complex technical operations and ultimately serve as the Agency's technical experts. Accordingly, it is critical that persons selected to be TSAs have the highest degree of technical knowledge, aptitude, and training. Generally, these persons must have long-term experience in conducting technical surveillance operations, telecommunications, and technical support.

12.5.c.(3). **Supervision.** The TSA is assigned to DCIS Technical Services Program and is supervised by the Program Director, Special Operations.

12.5.d. **Organization of the Technical Services Program.** Technical services responsibilities are generally divided into three levels: headquarters, field office, and TIE inventory custodian.

12.5.d.(1). **Headquarters.** The Program Director, Special Operations is responsible for the overall management of the DCIS Technical Services Program. The responsibilities of the DCIS Technical Services Program include complex technical surveillance operations, research and development, test and evaluation, TIE procurement, TIE inventory

management, and technical training. The DCIS Technical Services Program is led by a designated Program Manager and is staffed by SAs assigned as TSAs who perform full-time technical service duties. The TSPM serves as the account custodian of the Master TIE Account.

12.5.d.(2). **Field Office (FO).** The TSS assigned to the FO is the primary TSS for the FO and serves as the FO TIE account custodian—a sub-account of the Master TIE account.

12.5.d.(2).(a). Each FO SAC must designate a primary and an alternate TSS in writing to the AIGI, INV OPS upon assignment of duties.

12.5.d.(2).(b). When staffing, workloads, or experience levels dictate, the FO SAC may assign a TSS, other than the one at the FO, to serve as the primary or alternate TSS.

12.5.d.(3) **Resident Agency TIE Custodian (RATC).** The RATC assigned to an RA may perform technical duties for the RA and at subordinate posts of duty. The RATC is responsible for all TIE assigned to the RA TIE account—a sub-account of the FO TIE account.

12.5.d.(4). **Post of Duty TIE Custodian (PODTC).** The PODTC assigned to a POD may perform technical duties for the POD. The PODTC is responsible for all TIE assigned to the POD TIE account—a sub-account of the RA TIE account.

12.6. Technical Investigative Equipment (TIE)

12.6.a. **Storage and Security of TIE.** The collective inventory of TIE represents a considerable investment of resources that require appropriate protection. DCIS TIE at all levels must be secured in containers or rooms with limited access. Local TSSs, in coordination with their supervisors, should establish operating procedures to ensure the proper accountability of TIE when it is not secured within its assigned container or room. During operational or training use, the level of security afforded an item of TIE must be appropriate to the local circumstances. Generally, TIE should never be stored overnight in vehicles or in unlocked containers in hotel rooms. However, it is impossible to dictate the exact security procedure for every situation—common sense and good judgment should always be used to determine the appropriate security procedure during operational or training use.

12.6.b. **Training Use of TIE.** DCIS SAs are highly encouraged to familiarize themselves with all assigned TIE before its actual use during operational activity. Since this familiarization and training is authorized for improving DCIS technical operations, using government-procured expendable supplies (for example, batteries and digital media) is authorized. All DCIS SAs are authorized to use DCIS-owned TIE for training, upon supervisory approval, except as follows.

12.6.b.(1). TIE must not be used for any purpose that violates federal laws or Agency policy, or discredits the Agency.

12.6.b.(2). TIE used for intercept purposes must not be used without proper Agency authorization.

12.6.b.(3). TIE must not be used for commercial purposes.

12.6.b.(4). TIE must not be used by or loaned to other persons, including family members, except in accordance with paragraph 12.6.i.

12.6.b.(5). The use of TIE must not interfere with operational activity.

12.6.b.(6). TIE must be readily available should an operational need arise.

12.6.c. TIE Property Accounts and Custodians. The Master TIE Property Account is divided into seven parts--Headquarters and the six FOs. The DCIS TSPM serves as the accountable TIE property officer, responsible for the overall management of all TIE as well as directly responsible for Headquarters TIE. The Primary TSS at each FO serves as the TIE Account Custodian for their respective FO. RATC and PODTC serve as TIE account custodians for the assigned sub-accounts..

12.6.d. Annual Inventory and Certification. The Master TIE Property Account Custodian maintains a database in the Case Reporting and Information Management System (CRIMS) to track the location of all assigned TIE. The Master TIE Property Account Custodian will provide CRIMS inventory database access to all assigned TSS, RATC and PODTC for certification. The Primary TSS at each FO must certify the accountability of all items no later than September 30. Discrepancies should be resolved between the Master and the FO custodians and documented in accordance with IG Instruction 4140.1, "Property Management Program," January 3, 2007. The SAC/RAC or their designated official must conduct an inventory (spot check) of each office's assigned TIE inventory within their AOR on an annual basis. The individual conducting the inventory must, at a minimum, randomly select five items of TIE and verify all items are properly labeled and accounted for in CRIMS.

12.6.e. Transfer of Custodian Duties and Inventory Certification. Whenever a TIE Account Custodian is replaced or transferred, a comprehensive inventory of all assigned TIE must be completed. If possible, the incoming and outgoing custodians should complete this inventory jointly. However, in all cases, the incoming custodian must certify the accountability of all assigned TIE within 1 month of assuming those duties. When the new custodian serves as the FO TIE Account Custodian, the Master TIE Property Account Custodian will provide CRIMS access to the FO TIE account for certification. Discrepancies should be worked out between the Master Custodian and the incoming/outgoing FO custodians. All other custodians (RATC/PODTC) will receive access to a copy of their assigned TIE inventory maintained in CRIMS.

12.6.f. Lost or Damaged TIE. Lost or damaged (beyond repair) TIE must be reported to the Master TIE Property Account Custodian via DD Form 200 in accordance with IG Instruction 4140.1, "Property Management Program."

12.6.g. **Transfer of TIE.** Transfers of TIE between Headquarters and field elements must be documented using a Property Receipt, DCIS Form 58. The Master TIE Property Account Custodian will provide information copies of property receipts to the FO Property Account Custodian when permanent transfers of TIE are conducted directly between Headquarters and offices subordinate to the FO.

12.6.h. **Shipping TIE.** TIE should be shipped using only carriers that provide adequate tracking capability. Offices shipping equipment should record the shipment tracking number on their copy of the property receipt to assist in locating or documenting lost TIE. All TIE must be packaged for shipping in a manner that prevents damage during transit. Do not use crosscut paper shreds (the waste product from your office shredder) for packing materials because they contain oils and dust particles that tend to damage sensitive electronic components.

12.6.i. **Loan of TIE.** DCIS-owned TIE may be loaned, with appropriate approval, to other law enforcement agencies.

12.6.i.(1). Local supervisors may approve loans of TIE to other DCIS offices.

12.6.i.(2). FO SACs may approve loans of TIE to other federal law enforcement agencies.

12.6.i.(3). The Program Director Special Operations must approve loans of TIE to state and local law enforcement agencies.

12.6.i.(4). The DAIGI, INV OPS must approve loans of TIE to non-law enforcement agencies.

12.6.j. **Procurement of TIE.** The DCIS TSPM is responsible for determining DCIS TIE requirements after coordination and approval from the TRAC. Field elements should submit their individual TIE requirements to the DCIS TSPM for validation and prioritization during the budget and procurement process. The DCIS Technical Services Program uses a requirements-based validation process to establish the overall TIE requirements and priorities. Generally, the DCIS TSPM will centrally procure all TIE to obtain volume pricing and ensure equipment interoperability. In rare instances, to meet operational demands or for the economy of the government, field elements with prior approval of the DCIS TSPM, may procure TIE items using the government purchase card. Conversely, field elements should always procure expendable technical supplies (for example, batteries and digital media) locally, using their DCIS FO government purchase card.

12.6.k. **TIE Authorizations.** The selection and quantity of TIE is directly related to fulfilling the needs associated with the technical support core capabilities cited in paragraph 12.5.b.(3). As such, the basic Table of Allowance (TA) for an FO, RA, and POD is shown in Attachment A. This TA is not an inventory log and is intended only to show the suggested minimum equipment allowance for an FO, RA, or POD. In most cases, offices will have considerably more equipment assigned than is shown on the minimum equipment allowance. As

required by operational, staffing, or other necessity, the DCIS TSPM will authorize additional equipment. Additionally, PODs with only one assigned agent or offices co-located with other law enforcement agencies may receive less equipment.

12.6.1. **Repair of TIE.** The DCIS TSPM oversees the maintenance program for all DCIS TIE. Requests for repair should be submitted by e-mail or memo to the DCIS Technical Services Program. Emergency requests for TIE repair should be submitted by phone. Both routine and emergency requests must contain the following information:

- 12.6.1.(1). name of item;
- 12.6.1.(2). identifying information such as model, serial, and barcode numbers;
- 12.6.1.(3). a brief description of the malfunction or repair requirement; and
- 12.6.1.(4). if appropriate, any operational time constraints or associated issues.

12.6.m. **Disposal of TIE.** All excess TIE must be disposed of in accordance with IG Instruction 4140.1 “Property Management Program.” In most cases, TIE will be declared excess and disposed of locally and should not be shipped to Headquarters for disposal. The TSS will contact the DCIS TSPM for final disposition approval.

(b)(7)(E)

12.6.m.(2). **Hazardous Materials.** TSSs are responsible for contacting their closest Defense Reutilization and Marketing Office (DRMO) to determine, and follow appropriate disposal and reclamation procedures for, hazardous materials such as batteries or chemicals.

(b)(7)(E)

(b)(7)(E)

12.7. Technical Training and Safety. The DCIS TSPM oversees the training program for all TSAs and TSSs. As technology changes the DCIS TSPM will reevaluate TSS and TSA mandatory and annual training needs. At a minimum all TSAs and TSSs are required to attend the CESP and DPLE courses listed below. All requests for TSS training must be submitted to the DCIS TSPM for technical validation. FO training coordinators are responsible for protecting their FO TSS training needs and submitting them to for Federal Law Enforcement Training Center (FLETC) for scheduling.

12.7.a. Initial Training for Technical Support Specialists

12.7.a.(1). **Covert Electronic Surveillance Program (CESP).** CESP is a 2-week course taught at FLETC. The course provides the student with a basic overview of technical surveillance collection techniques and methods, legal issues, safety, and core capabilities required to perform assigned TSS duties. This course, or its equivalent, is required and should be completed as soon as possible. Requests to substitute equivalent training should be submitted to the DCIS TSPM.

12.7.a.(2). **Digital Photography for Law Enforcement (DPLE).** DPLE is a 2-week course taught at FLETC. The course provides the student with in-depth knowledge and hands-on training in multiple skills and techniques required to capture, process, and print law enforcement specific photographs. It is strongly encouraged that all TSSs complete this course as soon as feasible.

12.7.b. **Training for Technical Services Agents (TSA).** In addition to CESP and DPLE training the TSAs will complete equivalent annual continuing training to include but not limited to the following fields as determined necessary by the DCIS TSPM.

(b)(7)(E)

(b)(7)(E)

12.7.c. **Additional Technical Training.** TSAs must accomplish annual continual training and TSSs are encouraged to complete some form of annual continual education. Training should be applicable to assigned duties and strike a balance between new technologies, maintaining current capabilities and liaison. The DCIS TSPM may evaluate additional sources of continuous technical training.

12.8. Requesting Technical Support. Whenever technical support is anticipated, early informal coordination is encouraged. Requests for operational technical support from DCIS Technical Services Program must be on a Request Form 1 for approval by the DAIGI INV OPS, or delegated authority. An example Request Form 1 is in Attachment B.

12.8.a. **Required Information.** The following is an outline of the information required for DCIS Technical Services Program support.

12.8.a.(1). DCIS Case Title.

12.8.a.(2). DCIS Case Number.

12.8.a.(3) Case Open Date.

12.8.a.(4). A brief summary of the case.

12.8.a.(5). A generic description of the technical support required (for example, request audio, video, and tracking support from DCIS Technical Services Program).

12.8.a.(6). Legal assessment of Reasonable Expectation of Privacy (REP). Cite the opinion of the appropriate legal authority for this case. When appropriate, cite whether a court order is required (pen register, GPS tracking, certain video installations, etc.). This is usually the responsibility of the prosecutor for the investigation.

12.8.a.(7). The objective of the technical surveillance.

12.8.a.(8). Proposed date/duration of technical surveillance.

12.8.b. **Legal and Agency Authority.** The Technical Assistance Request does not rule out the need to obtain proper legal authorizations as prescribed in SAM Chapter 11 and by federal law. The TSA will advise and assist the case agent in these matters, and may obtain legal advice from the DoD Office of the Inspector General (OIG) Office of General Counsel (OGC).

(b)(7)(E)

ATTACHMENTS

<u>Attachment</u>	<u>Title</u>
A	TIE, Minimum Table of Allowance
B	Blank Sample Request for Technical Services Support
C	Sample Request for Technical Services Support (GPS)
D	Sample Request for Technical Services Support (Non GPS)

CHAPTER 13

INSPECTOR GENERAL SUBPOENA GUIDELINES

<u>Contents</u>	<u>Section</u>
General	13.1
Legal Authority for IG subpoenas	13.2
Policies	13.3
Procedures for Preparing a Request for an IG Subpoena <i>Duces Tecum</i>	13.4
Headquarters Procedures for Processing an IG Subpoena <i>Duces Tecum</i>	13.5
Serving an IG Subpoena <i>Duces Tecum</i>	13.6
Production of Records in Response to an IG Subpoena <i>Duces Tecum</i>	13.7
Procedures for Judicial Enforcement of an IG Subpoena <i>Duces Tecum</i>	13.8
Procedures for Canceling an IG Subpoena <i>Duces Tecum</i>	13.9
Procedures for Changing or Reissuing an IG Subpoena <i>Duces Tecum</i>	13.10
Procedures for Preparing a Request for a Testimonial IG Subpoena <i>Ad Testificandum</i>	13.11
Headquarters Procedures for Processing a Testimonial IG Subpoena <i>Ad Testificandum</i>	13.12

13.1. General. This chapter states the policies and procedures for obtaining and serving DoD Inspector General (IG) subpoenas and applies to all elements of the Defense Criminal Investigative Service (DCIS). The DoD Inspector General is authorized to issue two general types of subpoenas: subpoenas *duces tecum* (subpoenas for documentary evidence) and subpoenas *ad testificandum* (subpoenas seeking testimonial evidence). It is also possible to issue a “combined subpoena” to a single subpoena recipient—e.g. a subpoena *ad testificandum et duces tecum*, which seeks both testimony and documents from the recipient. Generally, the processes and procedures for obtaining and serving both types of subpoenas are the same, with a few minor differences. The balance of the chapter states the processes and procedures for obtaining and serving IG subpoenas, with additional comments where the process or procedure for each type of subpoena differs.

(b)(7)(E)

(b)(7)(E)

13.2. Legal Authority for Inspector General Subpoenas

13.2.a. **Subpoenas *Duces Tecum* (Documentary Evidence).** Section 6(a)(4) of the Inspector General Act of 1978 (IG Act), as amended, 5 U.S.C. App. 3, authorizes the OIG to require by subpoena the production of all forms of documentary evidence necessary to perform the functions assigned to the OIG by the IG Act. The term “documentary evidence” has been held to mean by both case law and OIG practice, to include any paper document and anything capable of being produced as a paper document; digital data (any of which can be printed); pictures; and videos, movies, and audio recordings, which can all be provided as printed transcripts. The phrase “documentary evidence” does **not** include objects; e.g., a computer, a gun, a file cabinet, a part, a first-article sample.

13.2.a.(1). IG subpoenas may be issued when: (1) an investigation has been initiated, (2) the records sought are relevant to the investigation in question, and (3) the document request is not overly broad or unduly burdensome. As a matter of practice, IG subpoenas are not issued in support of investigative projects, although in highly unusual situations, exceptions have been made to this restriction.

13.2.a.(2). Normally, subpoena authority will apply to the following four broad categories of records:

13.2.a.(2).a. **Business.** The Act authorizes the OIG to require production of any business record, even those not normally made available under the contract. Furthermore, records may be obtained from corporations and subcontractors who may not be subject to the audit clause provisions of a particular contract.

13.2.a.(2).b. **Personal.** An individual can be required to produce any records regarding his or her personal finances or other matters, including tax returns, bank statements, and employment records.

13.2.a.(2).c. **Financial Institutions.** Banks, credit unions, loan companies, and credit card companies can be required to produce the financial records of any customers. However, the Right to Financial Privacy Act of 1978, 12 United States Code (U.S.C.) 3401 et seq., if applicable, must be strictly followed. (See DCIS Special Agents Manual [SAM] Chapter 14 for instructions and restrictions concerning subpoenaing financial institutions.)

13.2.a.(2).d. **Governmental.** A state or municipal governmental body or agency may be issued an IG subpoena and required to produce relevant documents. IG subpoenas may not be issued to other Federal Government agencies; however, §6(a)(3) of the IG Act authorizes the IG to request information or assistance from any Federal governmental agency, which is the mechanism used to obtain such records. Bear in mind that, with regard to obtaining documents from within the Department of Defense (DoD), §6(a)(1) and §8 of the IG Act, as implemented by DoDI 7050.03, gives the OIG access to all records within or available to any part of the DoD. The only person who can deny the OIG access to DoD records is the Secretary of Defense, who has never chosen to exercise that authority.

13.2.a.(2).e. **Basic Subscriber Information From Telecommunication Carriers.** Although an special agent must have a search warrant to obtain the contents of electronic communications and remote computing, the Electronic Communication Privacy Act, 18 U.S.C. § 2703(c), requires providers to disclose to the Government, pursuant to an administrative subpoena, the following subscriber information:

- (A) name;
- (B) address;
- (C) local and long-distance telephone connection records, or records of session times and durations;
- (D) length of service (including start date) and types of service used;
- (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
- (F) means and source of payment for such service (including any credit card or bank account number).

No prior notice to the customer or subscriber is required, but before seeking a subpoena or warrant, the special agent should coordinate with the provider to officially request preservation of the information. The law, 18 U.S.C. § 2703(f), states that “upon the request of a governmental entity, [the provider] shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.” The period of retention is 90 days, “which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.” 18 U.S.C. § 2703(f)(2).

13.2.b. **Subpoenas *Ad Testificandum* (Testimonial Evidence)**. Section 8(i) of the IG Act authorizes the DoD IG to issue subpoenas for testimonial evidence in support of investigations and audits involving the programs and operations of the Department, with the following conditions:

“The Inspector General of the Department of Defense is authorized to require by subpoena the attendance and testimony of witnesses as necessary in the performance of functions assigned the Inspector General by this Act, except that the Inspector General shall use procedures other than subpoenas to obtain attendance and testimony from Federal employees.

A subpoena issued under this subsection, in the case of contumacy or refusal to obey, shall be enforceable by order of any appropriate United States District Court.

The Inspector General, through OGC, shall notify the Attorney General 7 days before issuing any subpoena under this section.”

13.2.c **Other Applicable Regulations, Directives, and Policy Guidance.**

13.2.c.(1). DoD Directive 5106.01, Inspector General, Department of Defense, dated April 20, 2012.

13.2.c.(2). DoDI 7050.03, Access to Records and Information by the Inspector General, Department of Defense, dated March 22, 2013.

13.2.c.(3). IGDINST 7050.9, Use of DoD IG Administrative Subpoenas in support of Audits, Evaluations and Investigations, April 14, 2011.

13.2.c.(4). DCIS SAM, Chapter 14, Inquiries at Financial Institutions.

13.3. **Policies**

13.3. Field office (FO) and resident agency (RA) supervisors and special agents are responsible for ensuring subpoena requests are prepared in accordance with this chapter before submitting them to the DoD IG Subpoena Program Office Policy and Programs Directorate, Investigative Policy and Oversight (IPO). Before preparing a written request, contact the Subpoena Program Office to discuss questions, unique circumstances, or difficult situations. A subpoena request that is not in compliance with this chapter and requires major revisions will be returned to the supervisory Resident Agent in Charge (RAC) for resubmission, with written guidance from the Subpoena Program Office.

CHAPTER 14

INQUIRIES AT FINANCIAL INSTITUTIONS

<u>Contents</u>	<u>Section</u>
General	14.1.
Regulations	14.2.
Policies	14.3.
Obtaining Information Under the Fair Credit Reporting Act	14.4.
Obtaining Information Under the Right to Financial Privacy Act	14.5.
Required Action Necessary To Comply With the Right to Financial Privacy Act	14.6.
Certification of Compliance Requirement	14.7.
Interagency Transfer of Financial Records	14.8.
Customer Civil Actions for Violations of the Right to Financial Privacy Act	14.9.
Obtaining Access to Financial Records Overseas	14.10.
Marking Information Received From Financial Institutions	14.11.
Retention of Documents	14.12.
Reimbursement of Financial Institutions	14.13.
Exceptions Permitting Disclosures by Financial Institutions	14.14.
Obtaining and Using Bank Secrecy Act Information	14.15

14.1. General

14.1.a. This chapter contains policies and procedures for obtaining information under the Fair Credit Reporting Act (FCRA) and the Right to Financial Privacy Act (RFPA).

14.1.b. The FCRA, Title 15, United States Code, Section 1681 (15 U.S.C. 1681), *et seq.*, was enacted in 1970 and is administered by the Federal Trade Commission. The FCRA regulates consumer reports prepared by consumer reporting agencies for employment information purposes, or for the extension of credit or insurance to individuals or families in their private capacity within the United States and its territories.

14.1.c. The RFPA, 12 U.S.C. 3401, *et seq.*, establishes limitations, rules, and procedures for obtaining financial records from financial institutions. This statute also sets forth penalties for Government and financial institution employees who violate the RFPA. Subpoenas directed to financial institutions that call for the production of financial records of its customers necessitate strict compliance with the RFPA.

14.1.d. Subject to the restrictions set out in this chapter, financial data information should be obtained on subjects, suspects, and other involved individuals or businesses whenever it could reasonably be expected to assist in the investigation. Financial data information may be

useful in tracing income and expenditures of a subject or suspect, in developing complete information on the subject's financial background, or for confirming or refuting statements or testimony.

14.2. Regulations

14.2.a. The FCRA, 15 U.S.C. 1681, *et seq.*, as implemented by regulations set forth in the Code of Federal Regulations (C.F.R.), 16 C.F.R. 600.

14.2.b. The RFPA, 12 U.S.C. 3401 *et seq.*, as implemented by regulations set forth at 12 C.F.R. 219 and 32 C.F.R. 275.

14.2.c. Currency and Foreign Transactions Reporting Act of 1970, 31 U.S.C. 5311, *et seq.*, and 31 C.F.R. 103.

14.2.d. DoD Instruction 5400.15, "Guidance on Obtaining Information from Financial Institutions," Change 1, July 3, 2007.

14.2.e. For definitions of terms used in this chapter relating to the FCRA and the RFPA, refer to Attachment A.

14.3. Policies

14.3.a. **Contracts With Credit Bureaus.** The number of investigations in which obtaining credit bureau reports is desirable and permissible will usually not be great enough to warrant entering into contracts with credit bureaus. However, if the credit bureau refuses to release any information without a contract and the Special Agent in Charge (SAC) or Resident Agent in Charge determines there will probably be a sufficient number of Defense Criminal Investigative Service (DCIS) requests under the contract to justify the expense, a contract may be sought. Submit a memorandum requesting funding action to the Special Agent in Charge, Internal Operations Directorate (SAC, INT), through the Special Agent in Charge, Investigative Operations Directorate (SAC, INV), Headquarters, DCIS.

14.3.b. **Requesting Reports.** If the consumer has given written permission, there is no need to explain the use that will be made of the consumer report. If the consumer has refused permission and an attempt is made to get a consumer report, the special agent must be prepared to explain the legality of the request; for example, the report will be used to determine the consumer's eligibility for a Government license or benefit as authorized by the FCRA. If requested by the consumer reporting agency, special agents are authorized to execute a written statement to the effect that the consumer report will be used for official purposes and that DCIS is authorized to receive it under the FCRA. If the special agent wants only identifying data on the consumer, there is no need to explain the intended use of the information to the consumer reporting agency.

14.3.c. **Penalties.** Since the FCRA provides harsh penalties for consumer reporting agencies that violate the law, such agencies may be reluctant to release any information to an

investigative agency such as DCIS. DCIS has no means to force the release of information, so special agents must rely on liaison to obtain information under circumstances wherein the FCRA permits it. The FCRA provides, “Any person who knowingly and willfully obtains information on a consumer from a consumer reporting agency under false pretenses shall be fined under title 18, or imprisoned for not more than 2 years, or both.”

14.3.d. Rights and Duties of Financial Institutions. Financial institutions are obligated to assemble records requested through administrative summons/subpoena or judicial subpoena even during the pendency of customer challenge proceedings. Financial institutions have the right to resist a Government request for records on various grounds (vagueness, undue burden) and such rights remain unaffected by the RFPA but cannot be asserted by the customer.

14.4. Obtaining Information Under the Fair Credit Reporting Act

14.4.a. Obtaining Consumer Reports. DCIS can legally obtain consumer reports from a consumer reporting agency only under the following circumstances.

14.4.a.(1). Consumer’s Written Permission. In an investigation where a consumer report is required or would be helpful and it cannot be legally obtained without the consumer’s written permission (see paragraphs 14.4.a.(2). and 14.4.a.(3).), the special agent should request that the individual concerned execute a written release if it would not jeopardize the security of the investigation. A release should also be requested when a consumer reporting agency that could legally release the information refuses to do so without a court order or written permission. Individuals must be advised that signing the release is voluntary on their part. Attachment B is a sample format for obtaining written permission applicable to consumer reporting agencies.

14.4.a.(2). Employment Purposes. Under the FCRA, a consumer report is used for “employment purposes” when it is used for the “purpose of evaluating a consumer for employment, promotion, reassignment, or retention as an employee” (15 U.S.C. 1681a(h)). It is DCIS policy that very few DCIS investigations are conducted for employment purposes. Investigations of DCIS contacts (sources) are not for employment purposes. Investigations in which it is believed the only action contemplated is a board hearing on the subject’s retainability in the Armed Forces will not be considered as being conducted for “employment purposes,” unless military commands provide a positive written statement to that effect.

14.4.a.(3). Eligibility for a License or Other Benefit. The FCRA does not define a “license or other benefit granted by a governmental instrumentality,” but it has been determined that security clearances are a license. Although DCIS does not conduct personnel security investigations (PSIs), it may be helpful to note that consumer reports on the subjects of PSIs may be requested.

14.4.a.(4). Court Order. Under the FCRA, a consumer reporting agency must furnish a consumer report in response to the order of a court having jurisdiction to issue such an order.

14.4.a.(5). **Grand Jury Subpoenas.** The use of grand jury subpoenas is another alternative available to the DCIS Special Agent.

14.4.b. **Information Available From Consumer Reporting Agencies**

14.4.b.(1). **Identifying Data.** At 15 U.S.C. 1681f, the FCRA specifically authorizes consumer reporting agencies to release to any Government agency a consumer's name, address, former addresses, place of employment, and former places of employment.

14.4.b.(2). **Credit Reports on Businesses.** Any type of credit report, including investigative reports, on any businesses may be released without restrictions.

14.5. Obtaining Information Under the Right to Financial Privacy Act. The RFPA prohibits any Agency or department of the United States from obtaining financial records from a financial institution and financial institutions from providing them to the Government unless access is permitted by one of the exceptions to the RFPA, or is accomplished by one of the following five methods mandated under the procedures.

14.5.a. **Customer Authorization.** Customers may authorize access to identified records by giving approval in writing. Such authorization is effective for only 3 months and is revocable at any time before the records are disclosed (12 U.S.C. 3402(1) and 3404, and 32 C.F.R. 275.8(b)). The authorization must state the customer's rights under the RFPA, and a customer may not be required to give an authorization as a condition of doing business with a financial institution. The authorization must identify the records sought and the purposes and agencies to which the records may be disclosed. Institutions must keep records of the agencies to which customer-authorized access is granted. These records are open to inspection by customers. Although the statute requires that the customer furnish the authorization directly to the financial institution, practical necessity dictates that DCIS directly obtain the authorization and deliver it to the financial institution on behalf of the customer. While there is no legislative history on this point, it is the view of the Department of Justice that the named account holder of a joint account may authorize Government access to the account (e.g., either spouse in connection with a husband and wife account or any partner in connection with a partnership account). Attachment C is a sample of a customer release to be used to obtain customer authorization for access to financial information. This customer authorization will be submitted to the financial institution along with the Statement of Customer Rights (Attachment D) and a Certificate of Compliance (Attachment E). (NOTE: The customer authorization should specify all agencies anticipated to require access and the purpose should be broadly stated.)

14.5.b. **Administrative Summons or Subpoena.** An administrative summons or subpoena is a judicially enforceable demand for records when issued by a Government authority that is authorized by some other provision of law to issue such process. The Office of the Inspector General of the Department of Defense (OIG DoD) subpoena is considered to be an administrative subpoena under this definition and shall be used in accordance with Chapter 13, "Inspector General Subpoena Guidelines," DCIS Special Agents Manual (SAM). In addition to the normal requirements for subpoenas set out in SAM Chapter 13, the RFPA customer

notification requirements must also be satisfied (12 U.S.C. 3402(2) and 3405). Refer to SAM Chapter 13 and the online Subpoena Manual cited therein for detailed guidance regarding compliance with the RFPA when using an OIG DoD subpoena.

14.5.c. Search Warrant. The RFPA established procedures for obtaining financial records by search warrant. Current law for obtaining a warrant has not changed, but under the RFPA the Government must, within 90 days after execution of the warrant for financial records, mail a copy of the search warrant together with the following notice to the affected customer(s):

“Records or information concerning your transactions held by the financial institution named in the attached search warrant were obtained by this [agency or department] on [date] for the following purposes:[]. You may have rights under the RFPA of 1978 (12 U.S.C. 3401 et seq.) (12 U.S.C. 3406(c)).”

Customer notice may be delayed and the bank prohibited from notifying the customer of the search if an ex-parte court order is obtained. In each instance in which this procedure is used, the SAC shall notify the SAC, Investigative Operations, of the date of execution for the warrant, location and identity of the financial institution, and the case control number.

14.5.d. Formal Written Request. The RFPA formal written request exception concerning the prohibition against obtaining financial records is designed to allow Government authorities such as the Federal Bureau of Investigation and the U.S. Attorneys Offices, which do not have authority to issue administrative summonses or subpoenas, to obtain records. The exception does not apply to DCIS (12 U.S.C. 3402(5) and 3408).

14.5.e. Judicial Subpoena. A Government authority may obtain financial records pursuant to a judicial subpoena only if the subpoena is authorized by law and there is reason to believe that the records sought are relevant to a legitimate law enforcement inquiry (12 U.S.C. 3402(4) and 3407).

14.6. Required Action Necessary To Comply With the Right to Financial Privacy Act. This section provides an abbreviated list of the actions required by special agents to comply with the RFPA. For detailed information, see Attachment F.

14.6.a. Determine whether the records sought are covered by the RFPA—do they pertain to an “account” (savings, checking, share, or loan account) of a “customer” (living person or partnership of five or fewer partners) obtained from a “financial institution” (bank, savings and loan, credit union, mortgage bank, finance company, or credit card issuer) where the “customer” maintains his/her account in his/her true name or an alias.

14.6.b. If the records are covered by the RFPA, access procedures will vary depending on the form of process used. Following are the major steps to be observed for the seven access mechanisms most often employed by DCIS to obtain covered records.

(b)(7)(E)

14.7. Certification of Compliance Requirement

14.7.a. Before protected records may be obtained under any authorized method of access, the SAC of the DCIS field office seeking access must submit to the financial institution a certificate stating that all applicable provisions of the RFPA have been complied with. Good faith reliance by the employees and agents of the financial institution on the Government certification of compliance absolves the institution of civil liability for any improper disclosure of records. Certification is not required when proceeding by grand jury subpoena, an excepted method of access.

14.7.b. The certificate of compliance should be presented to the financial institution only when all requirements of the RFPA have been satisfied. For example, if a customer notice were given in connection with a subpoena, the certificate of compliance would be presented to the financial institution only after the challenge period has passed without a customer challenge or after the court has dismissed a customer challenge.

14.7.c. The challenge period is a three step process: (1) customer notification, (2) service of the subpoena, and (3) action taken by the customer to quash the subpoena.

14.8. Interagency Transfer of Financial Records

14.8.a. The RFPA sets forth restrictions on the transfer of financial records among Federal departments and agencies. Those procedures are substantially different from restrictions found in the Privacy Act of 1974, 5 U.S.C. 552a.

14.8.b. Financial records may be transferred to another Federal agency under 12 U.S.C. 3412 only if an official of the transferring agency certifies in writing that there is a reason to believe the records are relevant to a legitimate law enforcement inquiry of the receiving agency. In addition, within 14 days after any transfer, the customer must be notified of the transfer unless the Government has obtained, in connection with its original access or at the time of the transfer, a court order delaying notice (see Attachment M for an example of the notice to customer of transferred information.)

14.8.c. Transfer restrictions do not apply to intradepartmental transfers (e.g., DCIS may transfer financial records to the USACIDC or DoD litigating officers without restriction). In addition, post-transfer notice is required only for transfers between Federal departments—the RFPA does not restrict transfer of financial records from state or local government agencies to Federal agencies or from Federal to state and local agencies. Neither does the RFPA cover transfers of financial records between a Federal agency and an agency of a foreign government. Also, account identification information obtained (Attachment N) is exempt from the post-transfer notice. The RFPA was amended in 1988, adding a provision that limits transfer of records obtained under the RFPA to the Department of Justice to only those documents relevant to violation of Federal criminal law, and their use only for criminal investigative or prosecutive purposes. This precludes the transfer of records obtained under the RFPA to the Fraud Section, Civil Division.

14.9. Customer Civil Actions for Violations of the Right to Financial Privacy Act

14.9.a. The RFPA, at section 3417(a), authorizes customers to file a civil action to recover damages for violations of provisions of the RFPA either by the Government or a financial institution. Section 3417(a) provides that any agency or department of the United States or financial institution obtaining or disclosing financial records in violation of the RFPA is liable to the customer in an amount equal to the sum of:

14.9.a.(1). \$100 without regard to the volume of records involved;

14.9.a.(2). any actual damages sustained by the customer as a result of the disclosure;

14.9.a.(3). such punitive damages as the court may allow, where violation is found to have been willful or intentional; and

14.9.a.(4). in the case of any successful action to enforce liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court.

14.9.b. A financial institution, its employees, and agents are absolved of liability for any violation of the RFPA, if good faith reliance is placed upon a Government certificate of compliance with the RFPA.

14.9.c. While a civil action against the Government is directed at and will be satisfied by the Government agency rather than the individual Government official involved, any court finding of a willful or intentional violation of the RFPA requires the initiation of a proceeding by the Merit Systems Protection Board to determine whether disciplinary action is warranted against the agent or employee who was primarily responsible for the violation.

14.10. Obtaining Access to Financial Records Overseas

14.10.a. Military contractors have headquarters operations within the United States and OIG DoD subpoenas, subject to the RFPA, may be used for service upon those financial institutions. However, access to financial records maintained by military banking contractors in overseas areas or other financial institutions located on DoD installations outside the United States, the District of Columbia, Puerto Rico, Guam, American Samoa, or the Virgin Islands is preferably obtained by customer consent. However, in those cases where it would not be appropriate to obtain this consent or where such consent is refused and the financial institution is not otherwise willing to provide access to its records, a military search authorization must be obtained from the appropriate military commander. The search authorization must include a description of the records to which access is sought, the general purpose for the access and must be based on sufficient probable cause information (see SAM Chapter 19, "Searches").

14.10.b. Access to financial records maintained by all other financial institutions overseas shall be sought according to local foreign statutes governing such access.

14.10.c. Release of such financial information within DoD and to other Federal agencies shall be on a strict need-to-know basis.

(b)(7)(E)

(b)(7)(E)

14.12. Retention of Documents. All documents relating to any requests for access made under the procedures of this chapter, including certificates of compliance, consents, and notices to a customer, shall be retained as a permanent part of the case file.

14.13. Reimbursement of Financial Institutions

14.13.a. Generally, the Government is not required to reimburse record custodians for the cost of complying with the Federal legal process. Rather, compliance with the legal process is viewed as an incident of citizenship or, in the case of commercial entities, a cost of doing business. The RFPA, however, requires Government authorities to reimburse financial institutions for the costs incurred in furnishing certain financial records of individuals and partnerships of five or fewer individuals in connection with law enforcement inquiries.

14.13.b. Reimbursements to financial institutions for costs incurred in locating, retrieving, reproducing, and transporting financial records obtained under the RFPa as prescribed at 12 U.S.C. 3415, implemented by regulations in 12 C.F.R. 219.3, Appendix A, will be made as follows:

14.13.b.(1). Search and Processing

Clerical/Technical, hourly rate—\$22.00
Manager/Supervisory, hourly rate—\$30.00

14.13.b.(2). Reproduction Costs

Photocopy, per page—\$.25
Paper copies of microfiche, per frame—\$.25
Duplicate microfiche, per microfiche—\$.50
Computer diskette—actual cost

14.13.c. Upon receiving notification for reimbursement from the financial institution, a memorandum requesting reimbursement will be submitted to the SAC, INT. The memorandum should include the costs incurred, the case control number of the investigation, reason for the reimbursement, and any documentation provided by the financial institution.

14.13.d. DCIS is responsible for costs incurred pursuant to DCIS activities up to the time that judicial process (a grand jury subpoena, a trial subpoena, or a search warrant) is used to obtain financial information. At that point, the proper litigating component becomes responsible for costs incurred pursuant to its activities (e.g., Department of Justice).

14.14. Exceptions Permitting Disclosures by Financial Institutions

14.14.a. Financial institutions are permitted to notify Government authorities of possible violations of law reflected in records within the custody of the institution. This is interpreted to permit financial institutions to disclose the nature of the offense suspected, the identity of the customer involved, the identifying numbers of the accounts in which records reflecting offenses are contained, the dates of the transactions in question, and other information as is necessary to enable law enforcement authorities to initiate an investigation of the suspected offenses. However, the financial institutions are not permitted to turn over or to verbally disclose the contents of financial records. Rather, the law enforcement agency investigating the offense can then obtain access to the financial records through a form of legal process authorized by the RFPa.

14.14.b. Because the RFPa contemplates that law enforcement authorities must proceed under the RFPa to obtain actual financial records required in the investigation and prosecution of suspected offenses reported by financial institutions, the information provided in the financial institution's report of crime must be sufficient to allow the Government authorities to meet the requirements that the RFPa sets out for access to records. Specifically, the Government must be able to "reasonably describe" the records sought and to issue a certificate of compliance as

required. Moreover, in issuing a certificate of compliance, the Government authority (DCIS) must have “reason to believe that the records sought are relevant to a legitimate law enforcement inquiry.” Such a description and determination can not be made and certified to on the strength of the financial institution’s unelaborated and unevaluated suspicions alone. Finally, because access to financial records may be sought by customer authorization (e.g., access to victims is required), names and addresses of all protected customers whose records contain evidence of the suspected offense must be supplied so that law enforcement authorities can see the customer authorization of disclosure.

14.14.c. Financial institutions may disclose financial records necessary to collect debts owed to the institutions or to process and administer Government loans.

14.14.d. Any information not derived from records protected by the RFPA that will assist the law enforcement agency may be freely disclosed.

14.15. Obtaining and Using Bank Secrecy Act Information

14.15.a. The Bank Secrecy Act (BSA), otherwise known as the Currency and Foreign Transactions Reporting Act of 1970, requires U.S. financial institutions to assist U.S. Government agencies to detect and prevent money laundering. Specifically, the Act requires financial institutions to keep records of cash purchases of negotiable instruments, file reports of cash transactions exceeding \$10,000 (daily aggregate amount), and report suspicious activity that might signify money laundering, tax evasion, or other criminal activities.

14.15.b. Financial data collected from financial institutions by the Financial Crimes Enforcement Network (FinCEN) under BSA has proven to be of considerable value in the investigation of procurement fraud, money laundering, terrorist financing, and other financial crimes investigations by law enforcement. When combined with other data collected by law enforcement and the intelligence communities, BSA data assists investigators in connecting the dots in investigations by allowing for a more complete identification of the respective subjects with information such as personal information, previously unknown addresses, businesses and personal associations, banking patterns, travel patterns, and communication methods.

14.15.c. When U.S. financial institutions report obligatory currency transactions under the BSA involving DoD personnel, DCIS may be provided the information for further scrutiny. The transaction reporting forms created by FinCEN to address specific financial activity are:

14.15.c.(1). Currency Transaction Reports (CTRs)

Currency Transaction Report (FinCEN 104)

Currency Transaction Report by Casinos and Card Clubs (FinCEN 103)

14.15.c.(2). Suspicious Activity Reports (SARs)

Suspicious Activity Report by Depository Institutions (TD F 90-22.47)

Suspicious Activity Report by Securities and Futures Industries
(FinCEN 101)

Suspicious Activity Report by Casinos and Card Clubs (FinCEN 102)
Suspicious Activity Report by Money Services Business (FinCEN 109)

14.15.c.(3). **Other Forms**

Money Services Business Registration (FinCEN 107)
Report of International Transportation of Currency or Monetary
Instruments (CMIR) (FinCEN 105)
Designation of Exempt Person (DOEP) (FinCEN 110)
Report of Cash Payments Over \$10,000 Received in a Trade or Business
(FinCEN 8300)
Foreign Bank Account Report (FBAR) (TD F 90-22.1)

14.15.d. With regard to SARs, 31 U.S.C. 5318(g)(2) prohibits a host of parties, to include employees of the Federal government, from notifying any person involved in the activity being reported on a SAR that the activity has been reported. This prohibition precludes DCIS special agents from disclosing the content of a SAR or the fact a SAR has been filed to any person involved in the transaction. However, this prohibition does not preclude, under Federal law, a disclosure, in an appropriate manner, of the facts that form the basis of the SAR, such as in an interview, as long as the disclosure does not indicate or imply a SAR was filed or the information is included on a filed SAR.

14.15.e. To preclude an unintentional disclosure of SAR information to “any person involved,” it is imperative that DCIS standardize its report writing convention to treat SAR information in a manner similar to confidential source information. The use of SAR information or the fact that a SAR has been filed on specific activity will not be acknowledged in the body of any DCIS investigative report, whether a Case Initiation Report, Case Summary Report, or Report of Investigation.

14.15.f. SAR information requires protection from disclosure and will be treated as a non-reportable investigative technique, as specified in SAM Chapter 28, “Investigative Reports,” in the same manner as Title III wiretaps, mail covers, undercover operations, and grand jury information.

(b)(7)(E)

14.15.g. No banner will be used at the beginning of the investigative report highlighting the BSA or SAR as the source of the information or indicating that such information is contained in the investigative report. If a special interest banner is required, ensure it is used in accordance with SAM Chapter 28 guidance.

14.15.h. The prohibition against disclosure can also raise special issues when SAR records are sought by subpoena or court order. The SAR regulations direct organizations facing

those issues to contact their supervisor, as well as FinCEN, to obtain guidance and direction on how to proceed. In several matters to date, government agencies have intervened to ensure that the protection for filing organizations and the integrity of the data contained within the SAR database remain intact.

ATTACHMENTS

<u>Attachment</u>	<u>Title</u>
A	Definitions of Terms Relating to the FCRA and the RFPA
B	Release Authority for Consumer Reporting Agency
C	Customer Consent and Authorization for Access to Financial Records
D	Statement of Customer Rights Under the RFPA of 1978
E	Certificate of Compliance With the RFPA of 1978
F	Detailed Information Concerning Customer Notice Requirements
G	Customer Notice
H	Customer's Motion to Challenge Government's Access to Financial Records
I	Customer's Sworn Statement for Filing a Challenge
J	Sample Notice to Customer of Delay of Notice (Inspector General Subpoena)
K	Sample Notice to Customer of Delay of Notice (Search Warrant)
L	Sample Notice to Customer of Emergency Access
M	Sample Notice to Customer of Transferred Information
N	Sample Format for Requesting Basic Identifying Account Data
O	Sample Report Narratives for Confidential Financial Information

ATTACHMENT A

DEFINITIONS OF TERMS RELATING TO THE FCRA AND THE RFPA

1. For the purpose of this chapter, the following definitions relate to the terms used in the Fair Credit Reporting Act (FCRA).

a. Person. Any individual, partnership, corporation, trust, estate, cooperative, association, Government or governmental subdivision or agency, or other entity (15 U.S.C. 1681a(b)).

b. Consumer. An individual (15 U.S.C. 1681a(c)).

c. Consumer Report. A consumer report is any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (1) credit or insurance to be used primarily for personal, family, or household purposes; or (2) employment purposes; or (3) other purposes authorized under section 1681b of title 12, United States Code. The term does not include (A) any report containing information solely as to transactions or experiences between the consumer and the person making the report; (B) any authorization or approval of a specific extension of credit directly or indirectly by the issuer of a credit card or similar device; or (C) any report in which a person who has been requested by a third party to make a specific extension of credit directly or indirectly to a consumer conveys his or her decision with respect to such request, if the third party advises the consumer of the name and address of the person to whom the request was made and such person makes the disclosures to the consumer required under section 1681m of title 12, United States Code.

d. Investigative Consumer Report. A consumer report or portion thereof in which information on a consumer's character, general reputation, personal characteristics, or mode of living is obtained through personal interviews with neighbors, friends, or associates of the consumer reported on or with others with whom he is acquainted or who may have knowledge concerning any such items of information. However, such information shall not include specific factual information on a consumer's credit record obtained directly from a creditor of the consumer or from a consumer reporting agency when such information was obtained directly from a creditor of the consumer or from the consumer (15 U.S.C. 1681a(e)).

e. Consumer Reporting Agency. A consumer reporting agency is any entity which, for mandatory fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports (15 U.S.C. 1681a(f)). A credit bureau is a consumer reporting agency, but the definition is broad enough to include any business that discloses any credit information on a consumer other than that information relating to its own dealings with that consumer. For example, a

department store may provide information concerning its dealings with a consumer without being considered a consumer reporting agency, but it cannot disclose any information in its files relating to the consumer's credit transactions with another individual or business without becoming a consumer reporting agency. However, if the store complies with the FCRA governing consumer reporting agencies, then it is free to disclose financial information concerning the consumer and third parties.

2. For the purposes of this chapter, the following definitions are related to the Right to Financial Privacy Act (RFPA).

a. Financial Institution. Any office of a bank, savings bank, card issuer as defined under 15 U.S.C. 1602(n), industrial loan company, trust company, savings association, building and loan, or homestead association (including cooperative banks), credit union, or consumer finance institution, located in the United States, the District of Columbia, Puerto Rico, Guam, American Samoa, and the Virgin Islands (12 U.S.C. 3401(1)). Although not added to the definition of financial institution, the RFPA as amended by Public Law 101-647 (Nov. 29, 1990) applies to "holding companies" (12 U.S.C. 3401(6)), "whose records should be considered those of a financial institution for purposes of the Act."

NOTE: The RFPA does not protect records maintained in foreign offices of financial institutions.

NOTE: Financial institutions not covered include bonding companies, credit bureaus, brokerage houses, Government lending agencies, small business investment companies, the U.S. Postal Service, and Western Union. Although credit card issuers are covered in the RFPA, businesses that issue credit cards to facilitate sales (e.g., oil companies and large department stores) are "financial institutions" only with respect to records related to credit card use—card sales or credit sales made other than pursuant to credit cards are not covered, as the businesses are not a "card issuer" with respect to such transactions.

b. Financial Records. An original of, a copy of, or information known to have been derived from any record pertaining to a customer's relationship with a financial institution (12 U.S.C. 3401(2)).

c. Government Authority. Any agency or department of the United States, or any officer, employee, or agent thereof (12 U.S.C. 3401(3)).

d. Person. Any individual or a partnership of five or fewer individuals (12 U.S.C. 3401(4)).

e. Customer. Any person or authorized representative of that person who utilized or is utilizing any service of a financial institution, or for whom a financial institution is acting or has acted as a fiduciary in relation to an account maintained in the person's name (12 U.S.C. 3401(5)).

f. Supervisory Agency. With respect to any particular financial institution, holding company, or any subsidiary of a financial institution or holding company, any of the following that has statutory authority to examine the financial condition, business operations, or records or transactions of that institution, holding company, or subsidiary: Federal Deposit Insurance Corporation; Director, Office of Thrift Supervision; National Credit Union Administration; Board of Governors of the Federal Reserve System; Comptroller of the Currency; Securities and Exchange Commission; Commodity Futures Trading Commission; Secretary of the Treasury, with respect to the Bank Secrecy Act (Public Law 91-508, Title I [12 U.S.C. 1951 et seq.] and subchapter II of Chapter 53, Title 31; state banking or securities department or agency (12 U.S.C. 3401(7)).

g. Law Enforcement Inquiry. A lawful investigation or official proceeding inquiring into a violation of, or failure to comply with, any criminal or civil statute or any regulation, rule, or order issued pursuant thereto (12 U.S.C. 3401(8)).

h. Protected Financial Records. An item in the account of an individual or covered partnership must meet the four following tests to be protected.

(1) It must be held by a specific financial institution.

(2) It must pertain to an individual's (or covered partnership's) utilization of the services of that institution.

(3) It must relate to an account maintained by that individual (or covered partnership) at that institution.

(4) It must relate to an account maintained in that individual's (or partnership's) true name.

i. Financial Records Not Protected

(1) Forged or counterfeit financial instruments.

(2) Records relating to an account established under a fictitious name.

(3) Records in the possession of an institution other than the institution at which the person maintains an account (e.g., a check or money order cashed for a noncustomer; bank surveillance photographs; contents of a safe deposit box sought pursuant to a search warrant or records pertaining to services that do not involve an account relationship).

(4) Services that include the sale of stock, performance of computer services, and other activities that do not involve a debtor-creditor relationship.

ATTACHMENT B

RELEASE AUTHORITY FOR CONSUMER REPORTING AGENCY

(Date)

(Place)

In connection with an official investigation, I, _____, hereby authorize and instruct any and all credit bureaus or other consumer reporting agencies* providing consumer reports or any business establishment having data concerning business and other transactions concerning me to furnish them to any special agent of the Office of the Inspector General, Department of Defense, who presents this authorization. This authorization specifically includes authority to release for examination and reproduction, without legal process, all pertinent records concerning me.

Special Agent _____ has advised me of the provisions of the Privacy Act of 1974. **

Witness:

Special Agent, Office of the
Inspector General, Department
of Defense

(Signature)

(Address)

* Specific name(s) of institutions or business may be set out if appropriate.

** Include this statement when requesting this authority in connection with a parent dependency investigation. In accordance with the Privacy Act of 1974, the dependent must be advised that he or she need not authorize the release of any financial data and cannot be compelled to do so; however, failure to do so could result in dependency benefits being terminated.

ATTACHMENT C

CUSTOMER CONSENT AND AUTHORIZATION
FOR ACCESS TO FINANCIAL RECORDS

I, _____, having read the
(Name of Customer)
explanation of my rights, which is attached to this form, hereby authorize the:

(Name and Address of Financial Institution)
to disclose these financial records:

to the Office of the Inspector General of the Department of Defense for the following
purposes(s):

_____.

I understand that this authorization may be revoked by me in writing at any time before my
records, as described above, are disclosed, and that this authorization is valid for no more than
3 months from the date of signature.

_____, 20____
(Date)

(Signature of Customer)

(Address of Customer)

Public Law Section 11404(a) of the Right to Financial Privacy Act, Title 12, United States Code,
Section 3404(a)

ATTACHMENT D

STATEMENT OF CUSTOMER RIGHTS UNDER THE RIGHT TO FINANCIAL PRIVACY ACT OF 1978

Federal law protects the privacy of your financial records. Before banks, savings and loan associations, credit unions, credit card issuers, or other financial institutions may give financial information about you to a Federal agency, certain procedures must be followed.

Consent to Release of Financial Records

You may be asked to consent to make your financial records available to the Government. You may withhold your consent, and your consent is not required as a condition of doing business with any financial institution. If you give your consent, it can be revoked in writing at any time before your records are disclosed. Furthermore, any consent you give is effective for only 3 months, and your financial institution must keep a record of the instances in which it disclosed your financial information.

Without Your Consent

Without your consent, a Federal agency that wants to see your financial records may do so ordinarily only by means of a lawful subpoena, summons, formal written request, or search warrant for that purpose.

Generally, the Federal agency must give you advance notice of its request for your records explaining why the information is being sought and telling you how to object in court. The Federal agency must also send you copies of court documents to be prepared by you with instructions for filling them out. While these procedures will be kept as simple as possible, you may want to consult with an attorney before making a challenge to a Federal agency's request.

Exceptions

In some circumstances, a Federal agency may obtain financial information about you without advance notice or your consent. In most of these cases, the Federal agency will be required to go to court to get permission to obtain your records without giving you notice beforehand. In these instances, the court will make the Government show that its investigation and request for your records are proper. When the reason for the delay of notice no longer exists, you will usually be notified that your records were obtained.

Transfer of Information

Generally, a Federal agency that obtains your financial records is prohibited from transferring them to another Federal agency unless it certifies in writing that the transfer is proper and sends a notice to you that your records have been sent to another agency.

Penalties

If a Federal agency or financial institution violates the Right to Financial Privacy Act, you may sue for damages or to seek compliance with the law. If you win, you may be repaid your attorney's fees and costs.

Additional Information

If you have any questions about your rights under this law, or about how to consent to release your financial records, please call the official whose name and telephone number appear below:

(Name)

(Address)

(Title)

(Telephone)

Office of the Inspector General
Department of Defense

ATTACHMENT E

**CERTIFICATE OF COMPLIANCE WITH
THE RIGHT TO FINANCIAL PRIVACY ACT OF 1978**

TO: _____

(Name and Address of Financial Institution)

FROM: Office of the Inspector General
Department of Defense

I hereby certify that the applicable provisions of the Right to Financial Privacy Act of 1978, Title 12, United States Code, Section 3401-3422, have been complied with as to the subpoena served on _____, 20____,
(Date)

for the following financial records of:

_____, 20____
(Date)

(Address)

(Name and Title of Official)

(Telephone)

Office of the Inspector General
Department of Defense

Pursuant to the Right to Financial Privacy Act of 1978, good faith reliance upon this certificate relieves your institution and its employees and agents of any possible liability to the customer in connection with the disclosure of these financial records.

Public Law 95-630, Section 1103(b) of the Right to Financial Privacy Act, Title 12, United States Code, Section 3403(b).

CHAPTER 15

GRAND JURY PROCEEDINGS

<u>Contents</u>	<u>Section</u>
General	15.1.
Federal Grand Jury Investigations	15.2.
Description and Function of a Federal Grand Jury	15.3.
The Grand Jury Subpoena	15.4.
Grand Jury Subpoena Acquisition/Serving	15.5.
Protection of Grand Jury Material	15.6.
Reporting Grand Jury Actions	15.7.
Safeguarding Grand Jury Material	15.8.
Disposition of Grand Jury Material	15.9.

15.1. General

15.1.a. This chapter provides information and guidance with regards to Defense Criminal Investigative Service (DCIS) involvement with Federal grand jury matters. Special attention should be given to the section addressing the protection of grand jury materials.

15.1.b. The grand jury process exists as primary security to the innocent against hasty, malicious, and oppressive prosecution. Under the Fifth Amendment to the Constitution, “No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury... .” Rule 7(a)(1) and (b) of the Federal Rules of Criminal Procedure (FED. R. CRIM. P.) requires prosecution by indictment of an offense punishable by imprisonment for more than 1 year unless indictment is waived. The Fourteenth Amendment does not require states to initiate criminal prosecutions by grand jury indictment.

15.1.c. It should be noted that a DCIS Special Agent may be involved with a grand jury in the development of additional information on an investigation. In accordance with FED. R. CRIM. P. 6(e), DCIS Special Agents working in support of an attorney for the Government (such as an Assistant United States Attorney (AUSA) in enforcing criminal laws are not to disclose to any unauthorized person any matter occurring before the grand jury. Presentations to and deliberations of grand juries are secret. A “knowing” violation of the grand jury secrecy rules may be punished as a contempt of court.

15.2. Federal Grand Jury Investigations

15.2.a. Federal grand jury investigations require special attention to the FED. R. CRIM. P., especially Rule 6, which establishes procedures for the purpose, operation, and control of information emanating from deliberation of the grand jury. Because of variances in the rules and procedures of state grand juries, this chapter shall be limited to the discussion of Federal grand juries. Special agents must depend on the guidance of prosecuting attorneys when the issue of

handling state grand jury material arises. The main concern of the special agents pertaining to their involvement in grand jury investigations should be the safeguarding of information produced by any grand jury. (This matter is discussed further in section 15.6.)

(b)(7)(E)

15.3. Description and Functions of a Federal Grand Jury

15.3.a. The grand jury must consist of between 16 and 23 jurors. An indictment, commonly referred to as a “true bill,” can be returned only upon the concurrence of 12 or more grand jurors. The term of the grand jury may vary from district to district; however, it could serve up to 18 months. Only the following persons may be present at a grand jury proceeding: the jurors, Government attorney, witness (who may be a special agent), interpreter (when required), and court reporter or an operator of a recording device. The counsel for a witness is specifically excluded.

15.3.b. The Federal grand jury functions as an investigative body under the direction of a United States Attorney, but is supervised by a Federal District Court. The scope of the investigatory powers of the grand jury is generally unlimited and a grand jury inquiry may be conducted on a very broad basis before it determines whether an indictment should be returned.

(b)(7)(E)

NOTE: Rule 501 of the Federal Rules of Evidence (re: Privileges) does apply to grand jury proceedings.

15.4. The Grand Jury Subpoena

15.4.a. FED. R. CRIM. P. 17 covers procedures governing the use of grand jury subpoenas. The subpoena can be an effective tool when properly used by the investigator. A preliminary

showing of reasonableness is necessary for the issuance and enforcement of the grand jury subpoena. [REDACTED]

(b)(7)(E)

[REDACTED] It must be emphasized that a grand jury subpoena is not a seizure within the meaning of the Fourth Amendment.

15.4.b. The grand jury may obtain by subpoena virtually all non-testimonial or non-communicative evidence without a violation of a person's Fifth Amendment rights. For example, the records maintained by an accountant for a client must be produced despite the client raising Fourth or Fifth Amendment claims to prevent the production of partnership records. There are three basic tests that must be satisfied for the issuance and enforcement of a grand jury subpoena:

15.4.b.(1). a subpoena may command only the production of evidence relevant to the investigation,

15.4.b.(2). the specification of evidence to be produced must be with reasonable particularity,

15.4.b.(3). production of records covering only a reasonable period of time may be required.

15.4.c. Caution should be exercised when serving a subpoena upon a financial institution or other similar public entity since Federal or state financial privacy laws or local banking practices may require the institution or entity to notify the owner/holder of the account or records. *See also* the Right to Financial Privacy Act of 1978, Title 12, United States Code (U.S.C.), section 3401, *et seq.*

NOTE: For a further discussion of the Right to Financial Privacy Act, see Special Agents Manual (SAM), "IG Subpoena Guidelines," Chapter 13, and "Inquiries at Financial Institutions," Chapter 14.

15.5. Grand Jury Subpoena Acquisition/Serving

15.5.a. Federal grand jury subpoenas are issued by a Federal District Court upon the request of an Assistant United States Attorney and may be served upon any person or entity within the jurisdiction of the United States. Subpoenas are issued to require the production of documents or objects or the requirement for testimony before the grand jury (Attachment A). The procedures for requesting a subpoena will vary from office to office. Attachment B is an example of a grand

jury subpoena request. A subpoena for records may be simple or complex, depending on the nature of the records required to satisfy the needs of the investigation. Samples of the type of records that can be subpoenaed are provided as Attachment C. This attachment is provided only as a guide and the investigation or the instructions of the prosecuting attorney must prevail.

(b)(7)(E)

15.5.c. When serving a subpoena, ensure that the subpoena is served on the person identified on the subpoena and that such service is properly recorded with regard to time and place. In all instances, the return of the subpoena relating details of the service must be accomplished in a timely manner.

15.5.d. When obtaining documents pursuant to a grand jury subpoena, the special agent should immediately prepare an inventory of the documents by listing them by type and number of pages. The inventory should also indicate which subpoenaed materials have not been supplied. The inventory should identify the case to which the documents relate and the return date of the subpoena. A copy of that inventory should be provided to the U.S. Attorney's Office at the earliest possible opportunity for filing with the subpoena request.

15.6. Protection of Grand Jury Material

(b)(7)(E)

15.6.b. In accordance with FED. R. CRIM. P. 6(e), grand jury proceedings are conducted in secret. As enunciated by the Supreme Court in *United States v. Proctor and Gamble Co.*,

356 U.S. 677, 681 (1958), maintaining the secrecy of grand jury proceedings is of paramount importance for the following reasons:

15.6.b.(1). to prevent the escape of those whose indictment may be contemplated;

15.6.b.(2). to ensure the utmost freedom to the grand jury in its deliberation, and to prevent persons subject to indictment or their friends from importuning the grand jurors;

15.6.b.(3). to prevent subornation, or inducement of perjury and tampering with the witnesses who may testify before the grand jury;

15.6.b.(4). to encourage free and unimpeded disclosures by persons who have information with respect to the commission of crimes; and

15.6.b.(5). to protect the innocently accused, who is subsequently exonerated, from disclosure of the fact that he has been under investigation.

15.6.c. In order to guarantee that the secrecy of the grand jury proceedings will be maintained, Rule 6(e) provides in pertinent part:

Unless these rules provide otherwise, the following persons must not disclose a matter occurring before the grand jury: (i) a grand juror; (ii) an interpreter; (iii) a court reporter; (iv) an operator of a recording device; (v) a person who transcribes recorded testimony; (vi) an attorney for the government; or (vii) a person to whom disclosure is made under Rule 6(e)(3)(A)(ii) or (iii). ...A knowing violation of Rule 6 ...may be punished as a contempt of court.

15.6.d. Documents and other grand jury material that are subject to the provisions of Rule 6(e) may be disclosed in the following circumstances.

15.6.d.(1). The courts may authorize disclosure of a grand jury matter, subject to time, manner, and any other conditions the court imposes, when the disclosure is preliminary to or in connection with a judicial proceeding, when there is a request by the defendant “who shows that a ground may exist” for dismissal of an indictment because of a matter that occurred before the grand jury. Courts may also authorize disclosure “at the request of the government if it shows the matter may disclose a violation of military criminal law under the Uniform Code of Military Justice, as long as the disclosure is to an appropriate military official for the purpose of enforcing that law.” A similar provision exists for the request of a government of a state, Indian tribe, or foreign country.

15.6.d.(2). A disclosure may be made to Government personnel who are considered by the attorney for the Government as necessary to assist that attorney in performing his or her duty to enforce Federal criminal law. Government personnel include not only DCIS Special Agents, but also employees of any Federal, state, Indian tribal agency, or foreign government who are assisting in the grand jury investigation.

15.6.d.(3). Attorneys for the Government may disclose grand jury material to other attorneys for the Government. “Attorney for the Government” under the FED. R. CRIM. P. means any Assistant United States Attorney or Department of Justice attorney working on criminal matters. Attorneys working for state or local governments as well as Assistant United States Attorneys, Department of Justice, Civil Division, are **not** included in the above exception to the Rule 6(e) prohibition against the unauthorized disclosure of grand jury material.

15.6.d.(4). An attorney for the Government “...may disclose any grand jury matter involving foreign intelligence, counterintelligence (as defined in 50 U.S.C. § 401a), or foreign intelligence information (as defined in Rule 6(e)(3)(D)(iii)) to any federal law enforcement, intelligence, protective, immigration, national defense, or national security official...” to assist the official in performance of that official’s duties. The disclosed grand jury information may only be used as necessary to conduct that person’s official duty. The attorney disclosing the grand jury information must file under seal a notice with the court in the district where the grand jury is convened, stating that such grand jury materials were disclosed and to what agency or department it was disclosed. This is a new exception to the disclosure rules that comes from the USA Patriot Act, PUB. L. NO. 107–56 (2001) (codified in scattered sections throughout the U.S.C.). Foreign intelligence is defined as:

15.6.d.(4).(a). “[I]nformation whether or not it concerns a United States person, that relates to the ability of the United States to protect against...actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; ...sabotage or international terrorism by a foreign power or an agent of a foreign power; ...or clandestine intelligence activities by an intelligence service or network of a foreign power or an agent of a foreign power;” or

15.6.d.(4).(b). “[I]nformation, whether or not it concerns a United States person, with respect to a foreign power or foreign territory that relates...to the national defense or the security of the United States; or the conduct of the foreign affairs of the United States.”

15.6.e. A witness who has appeared and testified before a grand jury is not under any obligation pursuant to Rule 6(e) to keep his grand jury testimony secret.

15.6.f. All recipients of material should become familiar with the provisions of Rule 6, with particular attention being paid to the “Exceptions” section of the rule. In essence, the Rule indicates that it is incumbent upon the individual special agent to whom disclosure has been made to ensure that further disclosure of grand jury material will be made in accordance with the letter and the spirit of the law, as well as the instructions of the prosecuting attorney authorizing the disclosure.

(b)(7)(E)

15.6.g. DCIS Special Agents should regard “any matter occurring before the grand jury” as secret under Rule 6(e). Below is a DOJ interpretation of what material constitutes “any matter

occurring before the grand jury.” The inclusion of the listed items in the working definition of “matters occurring before the grand jury” is not meant to be a concession that all items in these categories actually are covered by Rule 6(e). It is an inclusive definition that is designed to avoid any difficulty.

15.6.g.(1). Grand jury subpoenas, and documents and physical evidence obtained by means of grand jury subpoenas *duces tecum*. This includes items turned over to a Federal agent pursuant to a waiver of appearance by a prospective witness, whether or not it is actually presented to the grand jury, and whether or not the evidence existed prior to the issuance of the subpoena.

15.6.g.(2). Grand jury testimony.

15.6.g.(3). Summaries or reports of statements of witnesses obtained pursuant to, as a result of, or shortly after the issuance of a grand jury subpoena, regardless of whether the witness actually testified before the grand jury.

15.6.g.(4). Any event or occurrence that took place before the grand jury, including but not limited to: materials revealing the strategy or direction of the grand jury, the nature of the evidence produced, questions or views expressed by members of the grand jury or attorneys for the Government, anything about the grand jury’s deliberations, and identities of witnesses.

15.6.g.(5). Pleadings and orders filed in connection with a motion to compel testimony and other sealed pleadings filed in connection with the grand jury investigation. In this regard, note that Rule 6(e)(6), FED. R. CRIM. P., states that “records, orders, and subpoenas relating to grand jury proceedings shall be kept under seal to the extent and for such time as is necessary to prevent disclosure of matters occurring before a grand jury.”

15.6.g.(6). Government work product (e.g., internal memoranda) that refers to, summarizes, or otherwise describes matters occurring before the grand jury.

NOTE: Generally, Rule 6(e) usually does not govern the disclosure of documents obtained by means independent of the grand jury. This is true even when such documents have later been examined by the grand jury or made grand jury exhibits so long as disclosure of the documents does not reveal that they were exhibits.

15.6.h. Regarding books and records, it should be noted that many of the Federal courts have held that books and records do not become matters occurring before the grand jury merely because they were subpoenaed and reviewed by the grand jury, provided the documents were created for a purpose other than the grand jury. Questions arising with regards to such matters should be closely coordinated with the local AUSA in order to ensure compliance with local practices.

15.6.i. Special agents shall be alert to problems relating to interviews of potential grand jury witnesses prior to their appearance before a grand jury. In some instances, courts have ruled

that depending upon the circumstances involved, such interviews constituted grand jury material.

(b)(7)(E)

(b)(7)(E)

15.6.k. In order to avoid any doubts as to the origin of information that may later be made available for prosecution of a civil case or administrative sanctions, information in the possession of DCIS must be identified by preparing a comprehensive record with appropriate indices and descriptions indicating the origin of the information prior to its presentation to an AUSA for criminal prosecution. Thereafter, any related information obtained by DCIS apart from grand jury information should be similarly recorded and its independent source specified.

(b)(7)(E)

15.7. Reporting Grand Jury Actions

15.7.a. Using the guidelines set forth above, information obtained as a result of Federal grand jury action will be reported on the investigative report, the DCIS Form 1. However, a Form 1 containing grand jury material must be secured separately from those reporting non-grand jury materials. This will allow for proper dissemination of non-grand jury information while ensuring that control is exercised over the privileged material. It will also provide for appropriate dissemination of grand jury material without further administrative review. Every effort should be made to limit the dissemination of sensitive material in investigations involving the use of the grand jury prior to the close of the investigation. In accordance with the guidelines set forth in SAM Chapter 28, reports referring to or containing information relating to the grand jury must include the following title:

GRAND JURY MATERIAL - DISSEMINATE ONLY PURSUANT TO RULE 6(e)(3), FEDERAL RULES OF CRIMINAL PROCEDURE

15.7.b. When a grand jury is actively investigating a matter brought before it by DCIS and the special agent is about to receive grand jury material for the first time, the special agent must determine the level of protection that is to be afforded the material and the persons to whom authorized disclosure may be made from the United States Attorney or AUSA. It is recommended that the instructions from the attorney, both for the handling and disclosure of grand jury material, be in writing. When oral instructions are received from the prosecuting attorney,

they must be reported in a memorandum for the file, with the subject entitled: “**GRAND JURY INSTRUCTION/DISCLOSURE.**” Written instructions received from the attorney, or the memorandum prepared by the case agent that documents the attorney’s instructions, will be kept with the case file. If the DCIS element conducting the investigation reports to a field office, as in the case of a resident agency, a copy will also be sent to the field office. This is especially important since the interpretation of what documents constitute grand jury material and the method by which 6(e) material should be handled will vary from one Federal jurisdiction to another.

15.7.c. Rule 6(e) requires that the AUSA inform the court of the names of all Government personnel to whom grand jury materials have been disclosed. Normally this will include the case agent and the special agent who actually receives the materials (if different from the case agent). It will also include the names of any other Government personnel (including supervisory or administrative personnel) to whom disclosure is made directly by the AUSA or any special agent. Due to the intricacies of DCIS investigations and the size and complexity of DoD, it is generally beneficial to the criminal investigation to add the names of one or more supervisory personnel, to include the name of the DCIS HQ case control coordinator, to the grand jury list. The investigating agent will encourage the prosecutor to add the names to the list. Where appropriate, additional DCIS personnel may have to be added to the 6(e) list. At some point in time, the Government attorney controlling the presentation to the grand jury will submit a disclosure order to the court that will identify those persons who have access to 6(e) material generated during the course of the investigation. As a result of this requirement, records of persons within DCIS who have access to grand jury material must be maintained. The case agent will advise prosecutors of the need for supervisory or administrative personnel, including DCIS HQ personnel, to have routine access to grand jury material. Most attorneys will require actual names and positions. The instructions of the attorney with regard to the disclosure of actual grand jury material govern these disclosures.

15.8. Safeguarding Grand Jury Material

15.8.a. Wherever possible, grand jury material should be stored in a separate and secure room. Whether or not a separate room is available, **material must be stored in a secure container and isolated from other files containing non-6(e) material.** To prevent unauthorized disclosures, access should be limited to special agents assigned to the investigation. Complying with Rule 6(e) and preventing the unauthorized disclosure of grand jury material must, in all cases, be of prime consideration. In instances where a DCIS component holds numerous separately identifiable documents containing 6(e) material, an individual within the component should be designated as the Grand Jury Material Custodian. This person should maintain custody of all 6(e) material and a system of accountability should be initiated. This system must be in sufficient detail to identify the documents pertinent to each case and the identity of authorized personnel who have had access to the documents on any given date. **It should be noted that 6(e) and non-6(e) material from the same investigation will be stored separately.** Non-6(e) material will be stored with regular investigative files. **Release of the 6(e) material should only be made with the approval of the AUSA concerned and should be clearly and fully documented/reported.**

15.8.b. When it becomes necessary to include Federal grand jury information or material in a report, the Forms 1 containing grand jury material are to be stamped with or bear the warnings: “GRAND JURY MATERIAL - DISSEMINATE ONLY PURSUANT TO RULE 6(e)(3), FEDERAL RULES OF CRIMINAL PROCEDURE.” The warning should be stamped on the first and last page. Under no circumstances shall grand jury material be transmitted electronically. All such material must be transmitted via Certified or Registered Mail (return receipt requested) or through an authorized commercial mail carrier with tracking abilities to a specific person to whom disclosure has been authorized in accordance with the instructions of the prosecuting attorney. Grand jury material should be mailed in a double envelope: the inner one should be addressed to the specific person to whom disclosure has been authorized. It should also be marked or stamped with the above warning and with the admonition: “TO BE OPENED BY ADDRESSEE ONLY.”

15.8.c. Grand jury material that contains information relevant to the maintenance of good order and discipline within DoD and/or the Military Departments, identifies financial obligations owed to DoD or the Military Departments, and/or furnishes evidence of contractual impropriety involving a DoD-issued contract, is of direct interest to DoD. When DCIS Special Agents are aware of the existence of such material, it is incumbent upon the special agents to obtain this material, together with proper authorization from the AUSA, and a court order, if necessary, and to make it available to the appropriate DoD authorities at the earliest possible date.

15.9. Disposition of Grand Jury Material

15.9.a. Grand jury records will be handled in accordance with SAM Chapter 42, “Investigative Records Management,” and appropriate Federal regulations. However, grand jury records obtained during an investigation will be maintained at the office conducting the investigation. DCIS HQ will not maintain copies of grand jury records. The following procedures are an exception to the rule when handling an investigative case file that has grand jury material, e.g., grand jury records obtained while working special operations, undercover, or HQ-controlled cases:

15.9.a.(1). if it is necessary for the grand jury records to be retained/retired with the case file, attach a letter of disposition from the AUSA to the grand jury envelope;

15.9.a.(2). place the copies in an envelope clearly marked “6(e) Grand Jury Material,” in accordance with this chapter;

15.9.a.(3). complete the 6(e) list form to identify individuals on the grand jury list and staple/tape to the outside of the envelope.

NOTE: **ONLY** those individuals specifically identified on the 6(e) list have access to the envelope; therefore, exercise care when completing the form.

15.9.b. The field office is responsible for the following actions.

15.9.b.(1). The field office will maintain investigative case files with sealed grand jury material in its file room until the retirement process begins.

15.9.b.(2). The case agent shall contact the AUSA to determine disposition instructions/authority. In accordance with the written correspondence specifying the disposition from the AUSA, the case agent will do one of the following:

15.9.b.(2).(a). return the grand jury material to the originator;

15.9.b.(2).(b). shred the grand jury material; or

15.9.b.(2).(c). retain the grand jury material for a specified time. If the grand jury material is retained/retired with the case, send the material to DCIS HQ with the written correspondence of disposition from the AUSA. If DCIS HQ grand jury material is retained (e.g., in instances involving special operations or undercover operations, HQ-controlled cases, or when it is necessary to keep these records with the retired case file), the file is segregated in the file room until the actual time of retirement.

ATTACHMENT A

SUBPOENA TO TESTIFY BEFORE GRAND JURY

AO 110 (Rev. 06/09) Subpoena to Testify Before a Grand Jury

UNITED STATES DISTRICT COURT
for the

SUBPOENA TO TESTIFY BEFORE A GRAND JURY

To:

YOU ARE COMMANDED to appear in this United States district court at the time, date, and place shown below to testify before the court's grand jury. When you arrive, you must remain at the court until the judge or a court officer allows you to leave.

Place:	Date and Time:
--------	----------------

You must also bring with you the following documents, electronically stored information, or objects (*blank if not applicable*):

Date: _____

CLERK OF COURT

Signature of Clerk or Deputy Clerk

The name, address, e-mail, and telephone number of the United States attorney, or assistant United States attorney, who requests this subpoena, are:

PROOF OF SERVICE

This subpoena for *(name of individual or organization)* _____
was received by me on *(date)* _____.

☐ I served the subpoena by delivering a copy to the named person as follows: _____

_____ on *(date)* _____; or

☐ I returned the subpoena unexecuted because: _____

_____.

I declare under penalty of perjury that this information is true.

Date: _____

Server's signature

Printed name and title

Server's address

Additional information regarding attempted service, etc:

Print

Save As...

Add Attachment

Reset



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

February 12, 2015

MEMORANDUM FOR ALL DCIS SPECIAL AGENTS

SUBJECT: Interim Policy for Special Agents Manual (SAM) Chapter 15, Grand Jury Proceedings; Regarding Safeguarding Grand Jury Material

Effective immediately, this interim policy modifies guidance provided in SAM Chapter 15 regarding whether grand jury material must be kept in a locked container within a separate and secure room. SAM Chapter 15, paragraph 15.8.a currently states:

“Wherever possible, grand jury material should be stored in a separate and secure room. Whether or not a separate room is available, material must be stored in a secure container and isolated from other files containing non-6(e) material.”

This resulted in confusion whether a locked container was necessary to store grand jury material within a separate and secure room. In order to correct this, the language in paragraph 15.8.a is modified to read as follows:

“Wherever possible, grand jury material should be stored in a separate and secure room. If a separate room is NOT available, material must be stored in a secure container and isolated from other files containing non-6(e) material.”

This interim policy is in effect until it is rescinded or incorporated into the next revision of SAM Chapter 15. Any questions related to this policy should be directed to (b)(6), (b)(7)(C) Deputy Assistant Inspector General for Investigations, Investigative Operations, at 703-604-(b)(6), (b)(7)(C)

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

Deputy Assistant Inspector General
for Investigations



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

June 22, 2017
Ref: DODOIG-2017-000193

SENT VIA EMAIL

This is an interim response to your Freedom of Information Act (FOIA) request for a copy of the Defense Criminal Investigative Service (DCIS) Special Agents Manual. We received your request on December 31, 2016, and assigned it case number DODIG-2017-000193.

The Defense Criminal Investigative Service conducted a search and found the enclosed documents, which consist of the Special Agents Manual Table of Contents as well as Chapters 16 through 30, as responsive to your request. After carefully reviewing the records, I have determined that 206 pages of records are appropriate for release in full, copies of which are enclosed. Additionally, I have determined that 59 pages of records are appropriate for release in part, and that 241 pages of records are exempt from disclosure pursuant to:

- 5 U.S.C. § 552 (b)(5), which pertains to certain inter-and intra-agency communications protected by the deliberative process privilege;
- 5 U.S.C. § 552 (b)(6), which pertains to information, the release of which would constitute a clearly unwarranted invasion of personal privacy;
- 5 U.S.C. § 552 (b)(7)(C), which pertains to records or information compiled for law enforcement purposes, the release of which could reasonably be expected to constitute an unwarranted invasion of personal privacy; and
- 5 U.S.C. § 552 (b)(7)(E), which pertains to records or information compiled for law enforcement purposes, the release of which would disclose techniques and procedures for law enforcement investigations or prosecutions.

In view of the above interim response, you may consider this to be an adverse determination that may be appealed within 90 days of the date of this letter, however we recommend that you wait to submit any appeal until after a final response is sent to you. If you choose to appeal the interim release now, the appeal must be sent to the Department of Defense, Office of Inspector General, ATTN: FOIA Appellate Authority, Suite 10B24, 4800 Mark Center

June 22, 2017
Ref: DODOIG-2017-000193

Drive, Alexandria, VA 22350-1500, postmarked within 90 days of this letter, and reference the file number above. I recommend that your appeal and its envelope both bear the notation "Freedom of Information Act Appeal." Please be assured that you retain the right to appeal our final determination and, when we provide our final response, you will be afforded another 90 calendar days in which to appeal.

You may seek dispute resolution services and assistance with your request from the DoD OIG FOIA Public Liaison Officer at 703-604-9785, or the Office of Government Information Services (OGIS) at 877-684-6448, ogis@nara.gov, or <https://ogis.archives.gov/>. Please note that OGIS mediates disputes between FOIA requesters and Federal agencies as a non-exclusive alternative to litigation. However, OGIS does not have the authority to mediate requests made under the Privacy Act of 1974 (request to access one's own records.)

Please note that this office is continuing to process your FOIA request, and you will be provided responses on a rolling basis. If you have any questions regarding this matter, please contact Searle Slutzkin at 703-699-7520 or via email at foiarequests@dodig.mil.

Sincerely,



Mark Dorgan
Division Chief
FOIA, Privacy and Civil Liberties Office

Enclosure(s):
As stated

Investigations



DCIS Special Agents Manual

Delegation of Authority to Establish DCIS Policy, March 14, 2011

(A) = Administration (O) = Operations	Current Chapter Version	Interim Policy Updates	Archived Policy
Chapter 1 - Organization, Mission, Jurisdiction & Authorities (A)	March 2016		
Chapter 2 - Sensitive Investigations Program	Aug 2015	IP2-1 (Passing Security Clearances)	
Chapter 3 - Asset Forfeiture Program (O)	Apr 2011		
Chapter 4 - Interviews and Interrogations (O)	May 2011		
Chapter 5 - Rights Warning (O)	Feb 2012		
Chapter 6 - Statements (O)	Oct 2014		
Chapter 7 - Confidential Informants (O)	Oct 2011		
Chapter 8 - Surveillance (O)	Apr 2011		
Chapter 9 - Undercover Operations (O)	Jul 2011	IP9-1 (Hold Harmless) (FOUO)	
Chapter 10 - Emergency and Extraordinary (E&E) Funds (O)	Jul 2011		
Chapter 11 - Interception of Wire, Electronic & Oral Communications (O)	Jun 2011	IP11-1 (Fm 43)	
Chapter 12 - Technical Services Program (O)	Aug 2014		
Chapter 13 - Inspector General Subpoena Guidelines (O)	Aug 2014		
Chapter 14 - Inquiries at Financial Institutions (O)	Jun 2011		
Chapter 15 - Grand Jury Proceedings (O)	Feb 2013	IP15-1 (Safeguarding)	
Chapter 16 - Not in use			
Chapter 17 - Physical Evidence and the Crime Scene (O)	Aug 2011		
Chapter 18 - Evidence Custody System (O)	May 2011	IP18-1 (Cash) IP18-1 TAB A IP18-2 (ETS)	
Chapter 19 - Searches (O)	Jun 2011		
Chapter 20 - Arrests (O)	Jun 2011		
Chapter 21 - See IGINST 1432.1, Incentive and Honorary Awards Program			
Chapter 22 - Juveniles and Criminal Investigations (O)	May 2014		
Chapter 23 - Victim and Witness Assistance (O)	Sep 2012		
Chapter 24 - Protective Service Program (O)	June 2016		
Chapter 25 - Coordination of Remedies (O)	January 2017		Chapter 25 - 2011
Chapter 26 - Not in use			
Chapter 27 - Not in use			
			Chapter 28 - 2011

Chapter 28 - Investigative Reports (O)	May 2017		Chapter 28 - 2015
Chapter 29 - Not in use			
Chapter 30 - Alternative Work Schedules Program (A)	Apr 2011		
Chapter 31 - Not in use			
Chapter 32 - Defense Criminal Investigative Service Mission Briefs (O)	Apr 2011		
Chapter 33 - Radio Communications (O)	Aug 2014		
Chapter 34 - Not in use			
Chapter 35 - Not in use			
Chapter 36 - Motor Vehicles (A)	Apr 2016	IP36-1 (DTD Guidelines)	
Chapter 37 - Not in use			
Chapter 38 - Use of Force (O) (A)	Feb 2016	IP38-1 (Personally Owned Weapons)	
Chapter 39 - Badges and Credentials (A)	Jul 2014		
Chapter 40 - Cyber Crimes Program (O)	Jul 2015		
Chapter 41 - Training (A)	Jul 2014	IP41-1 (Required Training)	
Chapter 42 - Investigative Records Management (O)	Aug 2011		
Chapter 43 - Not in use			
Chapter 44 - Not in use			
Chapter 45 - Not in use			
Chapter 46 - Not in use			
Chapter 47 - Performance Management (A)	Jun 2011		
Chapter 48 - Accounting for Disclosure of Information from DCIS Records (A)	Apr 2011		
Chapter 49 - Not in use			
Chapter 50 - CRIMS (O)	Oct 2014	IP50-1 (Probation) IP50-2 (Top 100) IP50-3 (Digital Signatures) IP50-4 (CDP Reviews)	
Chapter 51 - Critical Incident Management (A)	Jul 2004		
Chapter 52 - Not in use			
Chapter 53 - Not in use			
Chapter 54 - Law Enforcement Availability Pay (A)	Mar 2007	IP54-1 (Travel Comp Time) (Comp Time for Travel Form)	
Chapter 55 - Inspections (A)	Dec 2016		
Chapter 56 - Bloodborne Pathogens and Tuberculosis (A)	Apr 2011	IP56-1 (Training Due Date)	
Chapter 57 - Polygraph Examinations (O)	Dec 2014	IP57-1 (Request Procedures)	
Chapter 58 - Health and Wellness Program (A)	Dec 2013	IP58-1 (PRA Frequency) IP58-2 (PT Hours)	
Chapter 59 - Voluntary Transfer Program (A)	Apr 2011	IP59-1 (Voluntary Transfers)	
For previous versions of SAM Chapters, see the Investigative Policy Program Manager			



CHAPTER 17

PHYSICAL EVIDENCE AND THE CRIME SCENE

<u>Contents</u>	<u>Section</u>
General	17.1.
Collection and Preservation of Physical Evidence—Basic Considerations	17.2.
Searching the Crime Scene	17.3.
Crime Scene Sketch	17.4.
Crime Scene Notes	17.5.
Detailed Search of the Scene	17.6.
Trace Evidence	17.7.
Tool Marks	17.8.
Firearms Evidence	17.9.
Body Fluids	17.10.
Standard Samples	17.11.
Fires and Explosions	17.12.
Searching the Outdoors	17.13.
Vehicle Searches	17.14.
Search of the Deceased	17.15.
Recovery of Other Physical Evidence	17.16.
Processing Evidence for Laboratory Examination	17.17.
Laboratory Analysis	17.18.

17.1. General

17.1.a. In connection with criminal investigations, physical evidence may be defined as “articles or material found in an investigation that will assist in the solution of the crime and the prosecution of the criminal.”

17.1.b. Evidence obtained during the investigation of a criminal case may be of great value in solving the crime: first, by reconstructing the crime; second, by assisting in identifying the criminal; and third, by destroying the alibi of the subject when apprehended. By means of physical evidence found at the scene of the crime, it is often possible to reconstruct the manner in which the crime was committed. It may be possible to positively identify the individual who committed the crime by means of the personal nature of the evidence found, such as fingerprints, clothing with special marks, or other such articles. Usually, an apprehended suspect will have an alibi of some sort intending to show that he or she could not possibly have been responsible for the crime because of being somewhere else. In such instances, certain physical evidence may serve to refute an alibi and place the subject at the scene of the crime.

17.1.c. In addition to being of tremendous value in solving the crime, evidence greatly assists in prosecuting the criminal in court by definitely demonstrating his/her complicity, without which successful prosecution would be difficult, if not impossible.

17.1.d. In considering evidence found at the scene of a crime, the investigator is confronted with two distinct types of evidence. First, there is fixed or immovable evidence such as footprints in soil, tire prints in mud or on paved highways, or latent fingerprints on immovable objects or on objects that are too bulky to remove readily. The other type of evidence is movable or removable evidence that can be discovered at the scene of the crime, properly preserved and identified, and later used either to assist in solving the crime or prosecuting the criminal in court.

17.1.e. The ultimate value of physical evidence is determined by how useful it is in verifying that a crime has been committed, identifying the person or persons who committed the crime, and exonerating all others who might have been suspected of the crime. This chapter discusses crime scene searches; crime scene sketching; and collecting, handling, preserving, examining, and marking for identification various types of physical evidence most commonly encountered. Evidence concerning photographs, fingerprints, documents, and casts and molds will not be specifically addressed in this chapter.

17.2. Collection and Preservation of Physical Evidence—Basic Considerations

17.2.a. 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, it is still necessary to take precautions immediately to protect the crime scene.

(b)(7)(E)

17.2.c. The investigator must be properly equipped in order to professionally and successfully process the scene of a crime for the presence and recovery of physical evidence. All Defense Criminal Investigative Service (DCIS) offices are furnished with Crime Scene Search Kits to use during crime scene searches.

17.2.d. Discovering and collecting physical evidence through meticulous and professional crime scene search methods and procedures can be irreparably negated through improperly containerizing the collected evidence. Take extreme care to ensure against loss of valuable physical evidence following collection. This loss is generally experienced through improper preservation procedures and sometimes from improper packaging and shipping procedures. Another section of this chapter will specifically address guidelines for appropriate storage and shipping containers.

17.3. Searching the Crime Scene

17.3.a. 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 or be notified of the crime. While the circumstances of the particular case will naturally govern the actions taken to preserve the physical evidence, the following are considered to be generally valid guides.

(b)(7)(E)

17.4. Crime Scene Sketch

17.4.a. The scene of a crime frequently reveals many clues that assist the investigator in solving the crime. Coincidental with the procedures of protecting the area of the crime from contamination or alteration by interested bystanders is a specialized technique known as a “crime scene sketch,” where 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 or determine the precise size 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 or evidence at the scene. In sketching crime scenes, the investigator shows the scene, specifies where evidence is found, shows objects and their relationship to one another, and outlines approaches or entrances to other structures. Besides supplementing photographs, sketches support, clarify, and augment written descriptions. Sketches may be either rough draft sketches or finished drawings. They serve to outline the evidential facts in an investigation by fashioning a clear reconstruction of the crime scene.

17.4.b. Sketch materials should be readily available in a portable kit. Sketch equipment might include nothing more than a paper pad, ruler, protractor, pencils, and compass. More advanced equipment used in either mechanical or architectural drawing may complement the basic kit and prove invaluable to the investigator.

17.4.b.(1). Use a soft pencil and graph paper for the rough sketch at the scene of the crime. 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.

17.4.b.(2). For the finished drawing, the investigator may need a drawing set, a drafting board with accessories, India ink, and a good grade of drawing paper, although this is not mandatory. A finished drawing is a specialized refinement of the rough draft sketch and is normally drawn to scale by a person skilled in mechanical or architectural drawings for courtroom presentation, as well as being used as an appropriate enclosure to the investigator’s report.

17.4.c. The crime scene sketch should portray those items that have a bearing on the investigation. Including unnecessary details may result in a cluttered or crowded sketch and hide or obscure essential or relevant items. A proper sketch provides a two-dimensional view of the pertinent area and important objects or points, is drawn to scale, and should include such noteworthy aspects of the crime as the body of the victim, any overturned furniture, spent bullets, empty cash boxes, and other relevant items. A legend or explanation of symbols used to identify objects in the sketch will permit considerable detail in a sketch covering a small area, since the various objects may be lettered and an explanation included in the legend. Excessive lettering in a sketch generally results in a crowded sketch and obscure essential items. Data that further authenticates a crime sketch includes the title, the assigned case number, office, identification of the victim or scene portrayed, location, date and hour made, scale of the sketch, and the name of the sketcher. (Attachments A and B represent a typical crime scene sketch.)

17.4.d. For investigative purposes, sketches are divided into three types: the sketch of locality, the sketch of grounds, and the sketch of details.

17.4.d.(1). The sketch of locality presents a map of the crime scene and its general environment, including nearby buildings and property, roads leading to the scene, bodies of water, and landmarks. Use road maps, topographic maps, and military maps to draw an accurate sketch.

17.4.d.(2). The sketch of grounds depicts the scene of the crime with its nearest physical surroundings. Such a sketch gives depth, dimension, and perspective to the crime scene area. Trees, rocks, ditches, creek beds, driveways, fences, and flower beds can be located in relation to items of importance as evidence.

17.4.d.(3). The sketch of details describes the immediate crime scene only and is frequently shown as a cross-projection. When it is desirable to portray three dimensions to allow better correlation of the evidential facts of the scene, use a projection sketch. This projection sketch of the scene of a room is like a drawing of a cardboard box whose edges have been cut and the sides flattened. (See Attachment B.)

17.4.e. Note the following when sketching crime scenes.

17.4.e.(1). Always determine the direction of the compass. Record it on the sketch.

17.4.e.(2). Do all the measuring yourself. Do not rely on others to give the measurements to you.

17.4.e.(3). Sketch only those items that are clearly relevant to the case.

17.4.e.(4). Never make changes on the original sketch after you have left the crime scene.

17.4.e.(5). Correlate your sketch with photographic coverage, being sure to show camera positions on the sketch.

17.4.e.(6). Submit the sketch as an enclosure to the investigative report.

17.5. Crime Scene Notes

17.5.a. The investigator's notes of a crime scene are the personal and most readily available record of observation made during the search and the 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 the details or content of the investigator's notes. The objective of crime scene note taking, however, is simple. The notes must be logical and written so that they will remain meaningful long after the incident.

17.5.b. Taking crime scene notes should begin with the investigator's assignment to the case and continue through the completion of the investigation. The notes should be recorded in chronological order of observation, which means they will not necessarily be in logical order as, at this stage of the recording process, it is important only that the notes are complete. The investigator will later reorganize the information while writing the formal report.

17.5.c. The following are the essential elements of information to be covered in the investigator's notes. However, the list is not intended to represent all the categories of data that may be useful and recorded.

17.5.c.(1). **Date, Time, and Location.** The date and time of the investigator's assignment to the case should be noted, as well as from whom and by what means the assignment was received. Note the exact time of arrival, exact location of the crime scene, light and weather conditions, names of individuals contacted, and names of other persons on the crime scene at the time of the investigator's arrival.

17.5.c.(2). **Detailed Description of the Victim and His/Her Clothing.** Include the name, age, height, weight, complexion, color of hair and eyes, and when possible, the Social Security number and date of birth of the individual. Describe outer garments as observed.

17.5.c.(3). **Wounds.** Include information such as the exact location of a wound or injury, its type, size, and in the case of a bruise, its color.

17.5.c.(4). **Crime Scene Description.** Record any damaged items, any apparent disturbance of the normal arrangement of furniture or other objects, and the presence of objects that seem unusual in the context of the scene.

17.5.c.(5). **Camera and Film Information.** As photographs are taken, make notes that include the "f" stop of the camera, film speed, shutter speed, focus distance, direction in which the camera was faced, flash (if used), object(s) or areas photographed, and time the photograph was taken.

17.5.c.(6). **Evidence Discovery/Location.** Describe the item, the time it was discovered, by whom, the exact place of its discovery, how it was marked, the type of container it was placed into, how the container was sealed and marked, and the disposition of the item after collection.

17.5.c.(7). **Missing Items.** Note the absence of items that would normally be associated with the type of crime, the area of the crime scene, or with any deceased victims, e.g., items of clothing missing from the victim's body that could not be located at the scene.

17.5.d. Notes are valuable, not only as an aid to accurately recall events to be testified to in court, but also to furnish the raw material for the written report. The details recorded during the investigation should anticipate both the written report requirements and the possibility of the investigator being questioned on a given point by attorneys or by the court. Unless a different notebook is used for each case, a looseleaf 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 looseleaf notebook is used, remove the pages applicable to a case to avoid the possibility of unauthorized disclosure of facts relative to other cases.

17.5.e. Secure the investigator's notes regarding a search in a safe place until the case is closed. They should be retained with the DCIS case file pending completion of possible litigation. Even if the suspect is convicted, there is always the possibility that an appeal will require the investigator's reappearance in court; therefore, like physical evidence, retain the notes until appeals have been exhausted.

17.5.f. In major cases where the amount of physical material is large and the search of the crime scene is very lengthy and involved, a portable tape recorder may prove valuable. By taping observations and findings, the investigator can include more data in the notes. When this is done, the tapes should be transcribed into a written record for the investigator's use in court and the tapes retained in the event the transcription is questioned.

17.6. Detailed Search of the Scene

17.6.a. Record the crime scene before any objects are collected or removed from it, with the obvious exception of medical assistance to injured persons.

17.6.b. Criminal investigators have suggested, recommended, and used various crime scene searching techniques. Regardless of the technique used, the basic objective of the search is to locate physical evidence related to the crime under investigation. Additionally, though 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 prevent error.

17.6.b.(1). The first priority is evidence that is being significantly deteriorated by time or the elements.

17.6.b.(2). Examine, photograph, record, and collect, as appropriate, all major evidence items, taking them in the order that is most logical, and considering the requirement to conserve movement.

17.6.b.(3). Make casts and lift latent prints from objects to be moved from the scene as necessary.

NOTE: Items should not be moved until they have been photographed and examined for trace evidence. Fingerprints should be lifted, or at least developed and covered with tape, before an object is moved.

17.6.b.(4). When a deceased victim is involved, process the items of evidence lying between the point of entry to the scene and the body, then conduct the detailed search of the deceased. After that search, the body may be removed and the search continued.

17.6.b.(5). After processing the obvious evidence, begin searching for and collecting additional trace material before dusting for fingerprints. After trace materials have been collected, begin searching for latent prints.

17.7. Trace Evidence

17.7.a. Dust, dirt, and debris that are associated with a crime scene are referred to as “trace evidence.” It consists of minute particles of matter found adhering to clothing, upholstery, window sills, floors, carpets, beds, in trouser cuffs or pockets, on bullets, or from any other source where its mere presence endows it with evidential value. Trace evidence may be classified as belonging to one of three groups of matter—of vegetable, animal, or inorganic origin—examples of which are as follows.

17.7.a.(1). Vegetable Origin

Leaves	Sugars
Pollen	Paper
Tobacco	Wood fibers
Textile fibers	Flower petals
Seeds	Fungus
Starches	Vegetable oils

17.7.a.(2). Animal Origin

Hair	Animal organisms
Feathers	Feces
Animal fats	Insects or portions thereof
Scales	Body/skin tissue
Blood	Silk fibers
Gelatins	Spider webs
Bone	Semen stains

17.7.a.(3). **Inorganic Origin**

Brick dust	Ink stains
Soil, dirt	Sand, quartz, etc.
Paint fragments	Ceramic particles
Fragments of metal	Asbestos
Nylon fibers	Glass fibers
Lead from pencils	

17.7.b. Trace evidence may either be left at the scene of a crime or carried away by the perpetrator. The intrinsic value of trace evidence depends on how nearly it falls into the following categories.

17.7.b.(1). Matter, which though common and widespread, has some individuality or characteristic. (Example: Leaves found in the trouser cuff of a suspect had minute specks of green paint on them. The burglarized house had been recently spray-painted with green paint. Although these leaves were common to the neighborhood, they had a unique characteristic.)

17.7.b.(2). Matter is found that is uncommon or sparsely distributed. (Example: Particles of charred lath were found adhering to the clothes of a burglar suspected of having burglarized a drugstore. Entrance had been made through an attic in which there had been a fire at some previous date.)

17.7.b.(3). Matter, even though common, is found in unexpected places. (Example: Minute metal turnings of copper alloy were found in the trouser cuffs of a drug clerk suspected of having broken open a safe in a certain foundry. If the suspect had been employed in a foundry, the evidence would have had far less value or none whatsoever.)

17.7.b.(4). A number of individual pieces of matter, although singly of low evidential value, when taken together may be of great significance. (Example: Debris adhered to the clothes of a man suspected of having raped a child consisted of insect parts, mice feces, three different kinds of feathers, four types of seeds, two different colors of dog hair, and parts of three different kinds of leaves. Particles of each category were found on the floor of an abandoned shack where the attack took place.)

17.7.c. In the course of searching the crime scene, all items that will not be removed should be examined very carefully and handled as little as possible to avoid loss, damage, or contamination of any trace materials adhering to the items. Any trace evidence discovered should be immediately removed, properly packaged, sealed, marked, and safeguarded until submitted for laboratory examination. Similarly, pay attention to items that will be removed and submitted for laboratory analysis. Record all such findings in the investigator's notes, as well as photograph before removal.

17.7.d. While some trace materials may be discovered in the investigator's search, other materials may only be detected through the laboratory examination process, particularly trace

evidence that may be found among sweepings taken from the crime scene. The general rule of evidence collection—of moving from the obvious to the hard-to-discern items—also applies to collecting trace evidence. After all discernible trace materials have been gathered, sweep or vacuum the critical areas of the crime scene, taking care to avoid destroying any possible latent prints. Take sweepings from separate or distinct areas of the crime scene. Pack and identify the accumulation from each area separately for laboratory examination purposes. (Example: Sweepings taken from the “point of entry” area at a crime scene should be collected, packaged, and marked separately from sweepings taken in the vicinity of a body.)

17.8. Tool Marks. Tool marks are particularly valuable evidence because they can frequently be proven to have a unique relationship with the item that made them. Impressions made by objects in metal are the highest quality of evidence because of the tendency of hard surfaces to retain even microscopic marks. Consequently, it is most desirable to remove any item or material containing tool marks in order that it may be submitted for detailed laboratory examination. If for some reason an article bearing marks or impressions cannot be moved, perform appropriate cast and mold procedures.

17.9. Firearms Evidence

17.9.a. 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 criminal trial. However, unless the firearms evidence obtained during the investigation is properly handled and packed, its value may be reduced considerably.

17.9.b. Firearms evidence found at the scene of a crime may consist of bullets, cartridge cases, or guns. The gun may be a pistol, revolver, shotgun, rifle, machine gun, or some other type of firearm. Each type of firearms evidence obtained requires its own special method of handling because of the type of laboratory examination that may be required.

17.9.c. Should the evidence be a spent or fatal bullet, use extreme care in handling it. The firearms examiner uses the minute microscopic scratches appearing on the side of the bullet for making comparisons with test bullets from suspected weapons; for this reason, no additional scratches or identifying marks should be placed on the side of the bullet, either by accident or by design. When a bullet is removed from a body during an autopsy or by a physician performing surgery on a suspect or victim, exercise caution in handling the bullet so that additional scratches will not be placed on it. The medical examiner, the pathologist, the person who may remove a bullet from a body, or the investigator who first finds a bullet at the scene of the crime should mark the evidence specimen by placing his/her initials or some other easily identifiable mark on the base of the bullet. Those identifying marks should be noted and recorded in the notes of the investigator who subsequently takes possession of the evidence specimen.

17.9.d. With cartridge cases found at the scene of the crime, a slightly different procedure is necessary. The firearms examiner reviews marks that are found near the base of the cartridge case such as the firing pin mark, the breech face markings on the primer, and the

extractor and ejector marks. Inasmuch as all of those characteristics appear near the base of the cartridge case, any identifying markings that are placed on the cartridge case should be near the front end of the case or, preferably, within the case itself.

17.9.e. Very carefully wrap both bullets and cartridge cases to prevent any extraneous markings during storage or while in transit to the firearms examiner. Separately wrap each bullet or cartridge case in a wad of clean, soft, absorbent cotton, and then place in a separate cardboard box with sufficient additional cotton added to prevent the evidence from shaking around. Then label the box itself with a description of the evidence and the name or initials of the individual who packed the box. Where possible, seal the package or box with a gummed label bearing the signed name or initials of the individual packing and sealing the box.

17.10. Body Fluids

17.10.a. Blood is the most commonly discovered body fluid at the scene of a crime. Collect fresh or at least liquid blood with a clean medicine dropper, place in a glass vial, and add saline. Liquid blood may also be collected by soaking it up with a clean white gauze pad or a clean white cotton cloth. If the blood has soaked into a porous material, dry the sample away from heat or sunlight. Dried blood on objects is best left alone, and the object sent to the laboratory. When this is not possible, scrape the dried blood from the object's surface with a clean knife, razor blade, or scalpel into a pillbox or a clean paper receptacle. In such cases, take separate scrapings from the surface immediately surrounding the stain, place in a separate container, and forward to the laboratory with the blood sample so as to determine whether the material from which the blood was taken affects the laboratory tests of the sample. If bloodstains are cut from a piece of cloth, include enough of the unstained fabric surrounding the stain with the sample to perform control tests.

17.10.b. Items that possibly contain seminal, urinary, or other stains should also be sent intact to the laboratory for examination whenever possible. If not, the above procedures for sending only a sample of the material apply.

17.11. Standard Samples

17.11.a. Standards are samples of materials collected from a crime scene that may be used as the basis for comparison with material that is later collected as evidence. Standards also refer to samples of material surrounding a bloodstain, etc., such as adjacent surface scrapings or unstained fabric that may influence laboratory test results.

17.11.b. Items that were apparently damaged or broken during the commission of a crime are particularly valuable as standards. Common standard materials are paint chips, glass slivers, bits of metal, and fibers. If any similar materials are later found on a suspect, such standards might prove invaluable in helping to link the suspect with the scene of the crime. Collect samples of material that may have transferred or adhered to the suspect, particularly specimens of an area likely to have been in the suspect's path of entry and exit, as well as fibers from carpets, etc.

17.11.c. Secure elimination finger and palm prints when appropriate from all persons who had legal access to the crime scene. If foot and tire tracks are collected during the search, also consider obtaining impressions from vehicles and persons who had legal access to the scene.

17.11.d. Collect standards before releasing the crime scene, 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, collecting excessive samples is the wisest course.

17.12. Fires and Explosions

17.12.a. 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. However, the detailed search involves some special considerations and problems. The fire or explosion may have been set to cover up another crime such as homicide, burglary, or theft; or it may have been set to destroy records or physical property so that the owner could collect from the insurance company. The basic problem facing the investigator in a fire or explosion is to determine whether a crime has been committed.

17.12.b. In searching a fire scene, be particularly concerned with discovering the point of origin. If there are several origins that have no logical explanation, it may be reasonably certain that the fire was set. Very carefully search known or apparent areas of origin and collect samples of any form of fuel or accelerant that may be discovered. Petroleum products and soil samples from areas where such products are suspected to have been used are of particular interest. When damage has been heavy, the origin of the fire or explosion usually may be discovered only by carefully removing surface debris.

17.12.c. Make a search for "trailers," which can be any form of combustible materials that would or did allow the fire to move from one area to another; and search for devices such as electrical timers, candles, and clockworks that may have been used to delay the ignition.

17.12.d. When an explosion has occurred, be concerned with the nature of the explosive material. If the explosive was lighter than air, as in the case of natural gas, the walls will be blown or bowed out near the ceiling. If the material was vapor, or heavier than air, the walls will be blown out near the floor. If the exploding material was a solid, with low-order burning characteristics, there will be a noted pushing effect and a gap in the force path wherever it passed large fixed objects, such as upright posts. High-order explosions (dynamite is a good example) create a local shattering effect at the center of the blast.

17.12.e. The nature of exploding material may give some indication of the type of containers and igniting device to search for; e.g., if a fire was set by using liquid petroleum, search specifically for the remains of any container(s) that might have held the liquid. Another point often overlooked in a liquid petroleum fire is that all of the fuel may not have been consumed. In the course of firefighting efforts, fuel residue may be washed and absorbed into surrounding charred material or be carried away with runoff water; thus, both charred materials and runoff water can be of significant evidentiary value.

17.16. Recovery of Other Physical Evidence. 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. The investigator who is dispatched to a hospital to interview a victim, or who searches for a suspect incident to apprehension, should be on the alert for any items that may be of significance or comparable with evidence obtained in the crime scene search. For example, obtain the clothing and shoes worn by a victim of an assault or attempted homicide for their possible importance in determining whether fabric remnants or footprints found at the scene might be traceable to the perpetrator. On the other hand, seize the clothing of an apprehended suspect if the time element, description, or already recovered evidence indicates that it may be the same clothing worn during the commission of the offense and therefore may produce trace evidence. Investigators should be aware that many jurisdictions require a search warrant prior to making such a seizure. On the other hand, a search warrant may not be required in instances where a custodial facility routinely requires the surrender of a prisoner's clothing on entry into the facility and other garments are issued for wear. In addition to clothing, and depending on the circumstances of the investigation, other evidentiary materials that the investigator should consider for collecting or preserving are:

- 17.16.a. blood samples;
- 17.16.b. hair samples (head, pubic, other);
- 17.16.c. firearms residue;
- 17.16.d. fingernail scrapings;
- 17.16.e. complete sets of finger and palm prints;
- 17.16.f. footprints;
- 17.16.g. handwriting exemplars; and
- 17.16.h. photographs of body marks, wounds, or bruises.

17.17. Processing Evidence for Laboratory Examination

17.17.a. The first consideration of the investigator is to prepare and ship evidence so as to avoid contamination or other change. The second consideration is properly identifying evidence so 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. Consider several aspects of identifying, handling, and marking physical evidence. The manner of

identification, as well as the specific location on the item, is 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, or on the 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.

17.17.b. In the event a particular item of evidence possesses unique characteristics, contact the servicing criminal laboratory for specific instructions. (Attachment C portrays proper packaging methods for transmitting evidence to the laboratory.)

17.18. Laboratory Analysis. The use of laboratory methods in the solution of crimes is of recognized importance. Investigators should know what facilities are available in the average scientific laboratory and be aware of the techniques used by laboratory technicians in order to be of assistance in solving a crime. It is not expected that the investigator become an expert in scientific subjects, but should know what the laboratory can do and how to submit physical evidence in such condition that a maximum amount of information can be obtained. An investigator should have sufficient knowledge of laboratory facilities to tell the technician what sort of examination is wanted and provide relevant facts to assist in the examination. The laboratory can furnish leads for the investigator, the results of which may frequently be used in court. Following are some of the more important types of laboratory examinations.

17.18.a. **Spectography.** Spectography is the science of measuring the wavelength of a substance. Every substance has a characteristic wavelength that is developed by the use of the spectrograph. The principal advantage of spectography is that results may be obtained from minute specimens. An example would be the small particles on knife blades or other tools that could be compared with the metal from burglarized safes, dirt from under fingernails, or many other particles of evidence. It should be noted, however, that once a particle is placed in the spectrograph, it is no longer available as physical evidence, since it is destroyed during the examination.

17.18.b. **Microscopy.** Microscopy is the examination of minute particles of evidence to determine constituents. Some of the particles frequently examined are hair, dust, soil particles, glass, and rope. There is one special field of microscopy that is known as petrography, or the examination of minerals and soils. Dust found on clothing may be compared with similar dust found at the scene of the crime. Such evidence is considered circumstantial but may be sufficient to assist in obtaining a conviction.

17.18.c. **Toxicology.** 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 whether death resulted from suicide or homicide. Poisons are divided into the following general groups:

- 17.18.c.(1). alcohol (wood-methyl),
- 17.18.c.(2). acids,
- 17.18.c.(3). alkalis, and

17.18.c.(4). alkaloids.

The general groups listed above are broken down into a large number of specific materials, such as cyanide, lead, arsenate, and others. Carefully preserve evidence recovered during investigations of suspected poisonings. Place samples in nonmetallic containers. Wrap such articles as dishes and spoons individually. Place powders and other solids in pillboxes and wrap securely. Place body organs and liquids in stoppered glass bottles or jars and seal. Place each item in a separate container. Label each container in order that it may be properly identified. In some cases it is possible to pack body organs in dry ice for transmittal. If the body was embalmed before the organs were removed, forward a sample of the embalming fluid with the organs in order that the toxicologist can perform a control test.

17.18.d. **Glass Fragments.** Broken or fractured glass found at the scene of a crime can frequently furnish important leads. Examining the broken glass may reveal the cause of the fracture as well as the direction from which the blow was struck; or if a bullet, the direction and angle from which it was fired. Glass, being flexible, will bend slightly under the influence of force. Since glass bends in the direction in which force is applied, causing the glass on the opposite side to stretch, and since glass will withstand more bending than stretching, it will break first on the side opposite that from which the force is applied. An examination of the edge of a piece of broken glass will reveal a number of curved lines, which are called stress lines. Stress lines are almost parallel to one side of the glass and perpendicular to the other side. The stress lines indicate the increase in stress in the glass until it breaks and are always perpendicular to the side that broke first.

17.18.e. **Invisible Radiations.** Infrared and ultraviolet light, although invisible, make it possible to examine evidence by using photographic and other technical materials that are sensitive to their radiations. Items such as secret writing, scars, semen stains, laundry marks, and some invisible stains fluoresce, i.e., give off waves of light that are visible when exposed to ultraviolet light. When matter of an evidentiary nature is brought out by this means, a photograph can be made of it. It is also possible to mark materials with powders that will later show, under ultraviolet light, whether a suspect has been in contact with a material so treated. Ransom money, locks, fireboxes, and similar objects may be treated with fluorescent materials. By later examining the hands of a suspect under ultraviolet light, it can be definitely established whether or not the suspect has handled any objects that have been treated with a fluorescent material. Through the use of infrared light and special infrared film, photographs may be taken in a darkened room. By this means it is possible to photographically show erasures, forgeries, and writings on charred documents that are not visible to the unaided eye. Where documents become illegible through art and abuse, differences occur between inks, dyes, and pigments that, to the eye, appear identical. Those differences become evident under infrared light. Obscure stains and irregularities on many materials can be photographed by infrared. Secret writing and the contents of sealed envelopes may also be brought out using this method.

17.18.f. **Firearms Identification.** A system of firearms identification has been developed making it possible to determine if a certain gun fired a certain bullet. This is accomplished by using a comparison microscope. In all firearms that are rifled, it has been found that each gun has considerable individuality in that the lands and grooves make a certain

mark on a bullet fired from a particular gun. By comparing an evidence bullet with a test bullet, the firing weapon can be determined.

17.18.g. **Restoration of Numbers.** Objects that bear identification numbers, such as revolvers, knives, automobile engines and parts, typewriters, computers, and instruments, are frequently encountered in investigations. Sometimes the numbers are not visible because the metal has been ground or beaten.

(b)(7)(E)

(b)(7)(E)

ATTACHMENTS

Attachment A—Crime Scene Sketch

Attachment B—Crime Scene Cross Projection (Sketch)

Attachment C—Proper Transmittal of Evidence

CHAPTER 18

EVIDENCE CUSTODY SYSTEM

<u>Contents</u>	<u>Section</u>
General	18.1.
Definitions	18.2.
Responsibilities	18.3.
Authorized Storage Cabinets/Evidence Storage Areas	18.4.
Evidence Tag (DCIS Form 15) and Evidence Custody Document (DCIS Form 14)	18.5.
Files and Records	18.6.
Submission of Evidence	18.7.
Cash Maintained as Evidence	18.8.
Offsite Storage Procedures	18.9.
Inventory Procedures	18.10.
Quarterly Evidence Accounting	18.11.
Transfer of Evidence	18.12.
Shipment of Evidence	18.13.
Required Authority for Final Disposition Action	18.14.
Disposition Procedures	18.15.
Laboratory Examination of Evidentiary Material	18.16.

18.1. General

18.1.a. It is the policy of the Defense Criminal Investigative Service (DCIS) that all documents, items, or materials physically obtained by a special agent from a citizen, agency, subject, victim, crime scene, or other location, or obtained via search warrant, Inspector General subpoena, or grand jury subpoena are presumed to have *potential* evidentiary value to DCIS by virtue of the special agent's acceptance, seizure, or removal of the items. Therefore, reasonable efforts must be made to provide physical security and controlled access to the items or materials that are in DCIS custody even if they have not been entered into the DCIS Evidence Custody System (ECS). Such items, however obtained, should be segregated and safeguarded in appropriate storage cabinets and/or containers, until such time they deemed of evidentiary value. However, cash and other valuable items obtained, but not yet deemed of evidentiary value, should be immediately safeguarded in accordance with applicable physical security requirements outlined in section 18.4. of this chapter until such time the determination of evidentiary value is made.

18.1.b. The unique nature of DCIS investigations, which frequently involve voluminous quantities of documents, requires a practical policy and feasible procedure for identifying, securing, and handling evidence. DCIS policy is that all documents, recordings, computer records, or similar items in DCIS custody are not necessarily considered evidence and need not necessarily be entered into the DCIS ECS at the time they are initially received. DCIS policy is

that a chain of custody must be established only when such items are determined by the assigned special agent or the cognizant Government attorney to have evidentiary value to a potential or pending criminal, civil, or administrative proceeding. Once it is determined that an item has evidentiary value, it should be safeguarded as evidence from that moment and appropriate protections must be provided to ensure the physical safety of and controlled access to the item. The special agent assigned to an investigation must ensure that the receipt of any item of evidence is promptly and accurately documented and entered into the ECS as soon as possible, in accordance with the procedures set forth in this chapter. It is the responsibility of all DCIS investigative personnel to take every precaution to preserve the integrity of evidence in its original condition.

18.1.c. Classified documents may be maintained in the ECS, if necessary, as long as all appropriate information security regulations are followed. However, the procedures of this chapter do not apply to Special Access Program documents or Sensitive Compartmented Information documents that are acquired as evidence. In such cases, the special agent should work with the Program Director, National Security (PD, NS), and the appropriate program security office to develop procedures that will adequately address the chain of custody issues for the documents. In the event the investigation concerns an undercover operation, coordination should be initiated with the Program Director, Special Operations (PD, SO).

18.2. Definitions

18.2.a. **Evidence.** Any item that is seized, collected, or surrendered to DCIS and that is deemed to be of evidentiary value in a potential prosecution in establishing the elements of an offense or the truth of the matter being investigated.

18.2.b. **Property.** Any item seized, collected, or surrendered to DCIS that does not meet the above definition of evidence or any item of which the status or importance is yet to be determined.

18.2.c. **Evidence Storage Area (ESA).** A secured, limited-access space designated by the Special Agent in Charge (SAC) that is used for the storage of evidence and any other items deemed appropriate by the SAC. Limit unescorted access to this area to the Evidence Custodian and the Alternate Evidence Custodian.

18.2.d. **Authorized Storage Container.** A General Services Administration (GSA) approved cabinet, Class 6 equivalent or higher, used for the storage of evidence.

18.2.e. **Evidence Tag (Attachment A).** The DCIS Form 15 that is used to identify an item placed into the ECS.

18.2.f. **Evidence Custody Document (Attachment B).** The DCIS Form 14 that is used to identify an item placed into the ECS and to record the chain of custody and final disposition action for the ECS item listed on the form. DCIS Form 14a is a continuation sheet of the chain of custody acknowledgements.

18.2.g. **Evidence Log (Sample Entry—Attachment C).** A bound book that is used to record the receipt, transfer, removal, and/or final disposition of all evidence. The beginning of the Evidence Log will contain date entries of all inventories, all changes of primary or alternate ECS Custodians, and all changes of lock combinations.

18.2.h. **Active Custody File.** A looseleaf notebook that contains copies of all active DCIS Forms 14. Maintain DCIS Forms 14 in the Active Custody File as long as final disposition of the ECS item has not occurred.

18.2.i. **Final Disposition File.** A looseleaf notebook, divided by calendar year, that contains DCIS Forms 14 (copies or originals, as applicable) for which final disposition of evidence has occurred.

18.3. Responsibilities

18.3.a. The Assistant Inspector General for Investigations—Investigative Operations (AIGI-INV) is responsible for overseeing the ECS within DCIS.

18.3.b. The SAC, Internal Operations (INT), will coordinate assistance to each field office (FO) SAC in procuring sufficient facilities and equipment for the proper custody and storage of evidence at the FOs, subordinate resident agencies (RAs), and posts of duty (PoDs).

18.3.c. The SAC, FO has the following responsibilities:

18.3.c.(1). reviewing FO/RA/PoD ECS procedures to ensure compliance with DCIS policy and the requirements of this chapter and participating in the operations of the ECS to the extent necessary to ensure compliance with regulations and policy;

18.3.c.(2). coordinating with the SAC, INT for the procurement of facilities and equipment necessary to meet the ECS requirements at subordinate FO/RA/PoDs, as outlined in this chapter;

18.3.c.(3). ensuring that all special agent(s) in subordinate offices obtain disposition authorization in accordance with the procedures outlined in section 18.14. when evidence is no longer needed and that all disposition actions are in accordance with the requirements of section 18.15.;

18.3.c.(4). initiating a referral, in accordance with the procedures outlined in INV Interim Policy No.: 2010-1, Disciplinary and Adverse Actions, into any incident involving the improper handling of evidence that, as a result, diminishes or eliminates the value or usefulness of the evidence in question or is a loss or theft of evidence.

18.3.d. The RAC has the following responsibilities:

18.3.d.(1). appointing, in writing, special agents to the position of ECS Custodian and Alternate ECS Custodian(s) at the RA and PoD(s);

18.3.d.(2). supervising appointed ECS Custodian and Alternate ECS Custodian(s);

18.3.d.(3). conducting unscheduled random reviews of the ECS at the RA/PoD and participating in the day-to-day operations of the ECS to the extent necessary to ensure compliance with regulations and policy;

18.3.d.(4). initiating an referral, in accordance with the procedures outlined in INV Interim Policy No.: 2010-01, Disciplinary and Adverse Actions, into any incident involving the improper handling of evidence that, as a result, diminishes or eliminates the value or usefulness of the evidence in question or is a loss or theft of evidence.

18.3.e. The ECS Custodian, or in his/her absence the Alternate ECS Custodian, has responsibilities that cannot be further delegated. The ECS Custodian is responsible for ensuring the following:

18.3.e.(1). evidence is inventoried, tagged with a completed DCIS Form 15, DCIS Evidence Tag, packaged, and marked for identification prior to acceptance of the item for storage;

18.3.e.(2). The DCIS Form 14, DCIS Evidence Custody Document, is completed prior to acceptance of the item for storage and updated at every change of custody;

18.3.e.(3). evidence is appropriately safeguarded and segregated;

18.3.e.(4). the Evidence Log, Active Custody File, and Final Disposition File are properly maintained;

18.3.e.(5). inventories of all ECS items are conducted as required by the procedures outlined in section 18.10.;

18.3.e.(6). the disposition of an ECS item is accomplished in accordance with the procedures outlined in sections 18.14. and 18.15.

18.3.f. The special agent obtaining or receiving evidence will be responsible for ensuring the following:

18.3.f.(1). the item is properly protected;

18.3.f.(2). receipts for items obtained/seized are provided when requested or required;

18.3.f.(3). the item is marked for identification, properly inventoried, packaged, and tagged with a DCIS Evidence Tag. The original DCIS Form 14 is attached;

18.3.f.(4). the DCIS Form 14 is completed as described in section 18.5.;

18.3.f.(5). the item is entered into the ECS without delay, or placed in designated temporary storage as outlined in sections 18.4. and 18.9.;

18.3.f.(6). when a stored item has served its purpose, authorization is expeditiously obtained for its final disposition in accordance with the procedures outlined in sections 18.14. and 18.15.;

18.3.f.(7). the item is returned to its rightful owner or otherwise disposed of in accordance with the procedures outlined in sections 18.5., 18.14., and 18.15.

18.4. Authorized Storage Cabinets/Evidence Storage Areas

18.4.a. Each FO/RA/PoD will establish an evidence repository. Questions regarding the cabinets and/or locking mechanisms required will be directed to the SAC, INT.

18.4.a.(1). Secure any container used for the storage of ECS items with the type of lock specifically described in this section.

18.4.a.(1).(a). Only a U.S. Government Class 6 cabinet that has been approved by GSA under Federal Specifications AA-F-358G or its equivalent or higher can be used as an ECS item container.

18.4.a.(1).(b). Lockbar-padlock variety and key lock filing cabinets are not authorized as ECS item containers.

18.4.a.(2). The ESA can be a closet or room that is used as a secure space for ECS item storage. The following specifications must be followed when constructing the ESA.

(b)(7)(E)

(b)(7)(E)

18.4.b. Turn over all items of evidence received, from whatever source, to the ECS Custodian for accountability and storage.

18.4.b.(1). Store items that the SAC, FO, deems to be sensitive ECS items (e.g., weapons, narcotics, money, jewelry, precious metals) in an authorized ECS cabinet as outlined in paragraph 18.4.a.(1).(a). If a weapon is too large to be stored in an authorized ECS cabinet, it may be stored in the ESA.

18.4.b.(2). When a cabinet has been designated for ECS items, no other materials or equipment will be stored therein unless each drawer of the cabinet has an individual lock, in which case ECS items will not be stored in the same drawer with non-evidentiary items.

18.4.b.(3). Store large volumes of ECS items in an ESA as described in paragraph 18.4.a.(2).

18.4.b.(4). When a room or closet is used to secure ECS items, the ECS Custodian, at his/her discretion and with supervisory approval, may store non-ECS items within the ESA. These items must be segregated from ECS items.

(b)(7)(E)

(b)(7)(E)

18.4.c. The appointed ECS Custodian will maintain strictly limited access to items stored in authorized ECS cabinets and to ESA.

(b)(7)(E)

18.4.d.(1). The use of an acceptable temporary storage container can preclude an ECS item from being stored in various locations within the FO/RA/PoD and will eliminate the necessity for the special agent to personally contact the ECS Custodian to obtain secure storage. The following temporary storage containers are satisfactory:

18.4.d.(1).(a). a large U.S. mailbox, secured to the floor or other portion of the office structure by the type of lock described in paragraph 18.4.a.(2).(a).;

18.4.d.(1).(b). one or more small clothing or gym type lockers, secured to a permanent structure. The combination lock should be attached to each locker in an unlocked or open position. The special agent, upon placing material into the locker, will secure the lock;

18.4.d.(2). the special agent placing an ECS item into a temporary storage facility will do so in accordance with the procedures outlined in sections 18.7. and 18.9.;

18.4.d.(3). the ECS Custodian should, if possible, check temporary storage containers on a daily basis. Any temporarily stored ECS item will be removed and entered into the ECS in accordance with the procedures outlined in sections 18.7. and 18.9.

18.4.e. All DCIS offices should make an effort to comply with the aforementioned physical requirements for their ESA. If full compliance is not possible, appropriate documentation detailing the attempt(s) and mitigating measures taken to comply will be maintained by the affected office. Further, the noncompliance and reason(s) for it must be documented in writing and provided through the SAC, FO, to the AIGI-INV.

18.5. Evidence Tag (DCIS Form 15) and Evidence Custody Document (DCIS Form 14)

18.5.a. DCIS Form 15, Evidence Tag, will be used to identify an ECS item placed into the ECS. Use of the Evidence Tag as described below adds to the integrity and authenticity of the ECS item and provides original collection notes that may be used as a basis for creating the DCIS Form 14 at a more convenient time and place. It may be used to ensure tamper-resistant

sealing of the bag containing the piece or component of evidence. Additional tamper-resistant evidence tape should also be used to ensure tamper resistance.

18.5.a.(1). The entries on the Evidence Tag will correspond to the applicable entries on the DCIS Form 14. Prepare and attach an Evidence Tag to each item that will be listed on the DCIS Form 14. When a number of items will be grouped together as one item on the DCIS Form 14, only one tag is required.

18.5.a.(2). Enter appropriate data on the Evidence Tag and DCIS Form 14 and in the Evidence Log at the time items or documents are determined to have evidentiary value. The face of the tag will show the item number, Evidence Log number, code (DCIS four-digit alphanumeric designator code for the FO or RA, e.g., 30PX), name of submitting special agent, detailed description of the article, and name of person from whom property was seized, if applicable. Complete descriptions are required, such as: 20 suspected false certifications on letterhead from XYZ Company, seized from the left bottom desk drawer of William Johnson, production manager, ABC Company.

18.5.a.(3). It is the responsibility of the case agent to ensure items entered into the ECS are properly tagged.

18.5.b. DCIS Form 14, Evidence Custody Document, is designed to establish the necessary control and maintenance of the chain of custody of ECS items while under the control of DCIS.

18.5.b.(1). This form will not be used to reconstruct the chain of custody of another law enforcement agency releasing items to DCIS. Such investigative activity will be accomplished by obtaining appropriate statements and/or copies of the releasing agency's custody documents and attaching them to the newly completed DCIS Form 14. This does not preclude non-DCIS personnel who deliver items to DCIS from marking the item itself or the item's container for future identification.

18.5.b.(2). DCIS Form 14 is a two-sided form. The form consists of an original, two carbon copies, and a carbon-copied Evidence Property Receipt (Attachment D). DCIS Form 14(A) is a continuation sheet for the chain of custody acknowledgements and should be affixed to the original DCIS Form 14 and a photocopy affixed to the receipt maintained in the Active Custody File. Complete the form as follows.

18.5.b.(2).(a). **Office.** Insert the DCIS four-digit alphanumeric designator code for the FO or RA (e.g., 30PX).

18.5.b.(2).(b). **Case Control Number.** Insert the unique case control number (e.g., 201001234D).

18.5.b.(2).(c). **Log Number.** The ECS Custodian will enter the Evidence Log number.

18.5.b.(2).(d). **Date and Time of Seizure.** Self-explanatory.

18.5.b.(2).(e). **Name of Person From Whom Property Seized.** Self-explanatory.

18.5.b.(2).(f). **Location Where Property Seized.** Self-explanatory.

18.5.b.(2).(g). **Case Title.** Enter case title.

18.5.b.(2).(h). **Item.** Use letters A through Z for each item listed; thereafter, use AA through ZZ.

18.5.b.(2).(i). **Quantity.** List items with different serial numbers, model numbers, identifying marks, values, etc., separately. Identical items may be grouped together.

18.5.b.(2).(j). **Disposition Action.** Upon disposition of an ECS item, the ECS Custodian will enter a number and letter code by each item to indicate the person receiving the ECS item or witnessing the action and the type of action. The number and letter codes are found in the Final Disposition Action section on the reverse side of the DCIS Form 14.

18.5.b.(2).(k). **Description of Property.** Give a complete description of the article. Include all information requested on the DCIS Form 14, as applicable.

18.5.b.(2).(l). **Name and Signature of Witness.** Self-explanatory.

18.5.b.(2).(m). **Name and Signature of Receiving Special Agent.** Self-explanatory.

18.5.b.(2).(n). **Chain of Custody.** This section will be completed by all personnel obtaining custody of ECS items in accordance with the procedures in this chapter.

18.5.b.(2).(o). **Final Disposition Authority.** This section (reverse side of form) will be signed by the appropriate authority, or authority will be granted in writing prior to final disposition of ECS item(s), in accordance with the procedures set forth in section 18.14.

18.5.b.(2).(p). **Person Receiving Item/Witnessing Destruction.** This section (reverse side of form) should be completed by the recipient of the ECS item or by the person witnessing the destruction.

18.5.b.(3). Carbon copies of the DCIS Form 14 will be placed in the Active Custody File and the case file. A photocopy will also be provided to the case agent. Photocopies of any updates to the original DCIS Form 14 will be made as needed.

18.5.b.(4). The Evidence Property Receipt (the last page of the DCIS Form 14) may be used as a receipt for property obtained and/or seized, when appropriate.

18.5.b.(5). If the space provided on the DCIS Form 14 for listing ECS items obtained is insufficient, list additional items on a second DCIS Form 14 and secure the two together. The first three lines should be completed on the second document in the same manner as on the first, and at the top right side of the form, write “page # of # pages.”

18.6. Files and Records

18.6.a. Store the Evidence Log, the Active Custody File, and the Final Disposition File in an authorized ECS cabinet/ESA. (b)(7)(E)

(b)(7)(E)

18.6.b. Each ECS Custodian will maintain the following ECS files and records in addition to the DCIS Forms 14.

18.6.b.(1). Maintain the Evidence Log in a hardbound logbook. The ECS Custodian will record ECS transactions only in the Evidence Log. Each DCIS Form 14 received by the ECS Custodian will be noted on a separate logbook line, regardless of how many items are listed on the DCIS Form 14. **The Evidence Log will also contain date entries of all inventories, all changes of ECS Custodians and Alternate ECS Custodians, and all changes of lock combinations.** Each entry indicating a receipt of an ECS item by the ECS Custodian will be assigned an Evidence Log number that will consist of two groups of numbers separated by a hyphen (-). The first group is a four-digit number issued sequentially as DCIS Forms 14 are received during a calendar year. The second group will be the last two digits of the calendar year, e.g., 0001-10 for the first DCIS Form 14 received during calendar year 2010; 0002-10 for the second DCIS Form 14, etc. Additional information for local control purposes may also be entered after the above items, if desired. Each entry will be made in blue or black ink on the next blank line and no empty lines will be permitted. In the event that an error is made in the entry, the entry should be lined through and marked with the Custodian’s initials. Erasures of entries are not authorized. The Evidence Log will be maintained for 5 years from the date of the last entry. It is presumed that the hardbound volume will serve for a number of years prior to starting a new volume.

18.6.b.(2). The Active Custody File will consist of a carbon or photocopy of the original DCIS Form 14 for the ECS item that has been received by the Custodian and for which final disposition has not occurred. This record will be maintained in one or more looseleaf notebooks. File the DCIS Forms 14 by Evidence Log number with new entries being placed on top. This record will then serve as a control device for periodic review of ECS holdings for possible disposition and will represent all ECS items for which the ECS Custodian is responsible. In the event storage bins or shelves are used in the ESA, the storage location (e.g., shelf #1, bin #3) will be entered in pencil on the DCIS Form 14 in the far left-hand margin next to the appropriate line number or at the end of the line on which the property is identified. The Active Custody File will be maintained as long as there is an ECS item in custody for which final disposition has not occurred.

18.6.b.(3). Maintain the Final Disposition File for all DCIS Forms 14 relating to an ECS item for which final disposition has occurred. This file will be kept in a looseleaf

notebook with dividers for each calendar year in which final disposition of an ECS item has been made. The original DCIS Form 14, except when it has been transferred to another investigative agency or DCIS office, will be filed in the Final Disposition File in chronological order of final disposition with the most recent entries filed on top. In the event the original is forwarded with the ECS item to another agency/DCIS office and the transfer is considered the final disposition action, a photocopy of the completed DCIS Form 14 will be placed in the Final Disposition File. The Final Disposition File will be maintained for a period of 5 years after the close of the calendar year covered by the file, at which time the DCIS Forms 14 will be destroyed.

18.7. Submission of Evidence

18.7.a. Promptly submit all items determined to have evidentiary value in a potential prosecution to the ECS Custodian. Do not retain physical control and custody of evidence longer than necessary to transport it to the FO/RA. Prepare the required documentation and submit the material to the ECS Custodian or, if necessary, place the evidence in temporary storage. Under normal circumstances, evidence will not be stored in a desk, administrative file cabinet, or vehicle. Evidence collected by DCIS at locations remote from a DCIS ESA 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 FO/RA/PoD by registered mail or other commercial shipment entity (e.g., Federal Express). Upon submitting an item to the ECS Custodian:

18.7.a.(1). ensure the item is properly marked for identification, tagged, and placed in an appropriate container, if needed;

18.7.a.(2). ensure the DCIS Form 14 is accurate and completed as described in paragraph 18.5.b.(2). The releasing special agent will sign the appropriate “Released By” block in the “Chain of Custody” section of the DCIS Form 14 and will note the reason for the release in the “Purpose” block; and

18.7.a.(3). if the special agent is placing the item in a temporary ECS storage container, securely attach the original DCIS Form 14 to the item deposited. The ECS Custodian upon receipting for the item and assigning an Evidence Log number will return a photocopy of the DCIS Form 14 to the special agent.

18.7.b. Upon obtaining custody of evidence, the ECS Custodian will:

18.7.b.(1). ensure the item is properly marked for identification and tagged in accordance with the procedures outlined in section 18.5.;

18.7.b.(2). examine, count, and weigh, as appropriate, all items identified on the DCIS Form 14 to ensure accuracy and accountability; and

18.7.b.(3). sign the appropriate “Received By” block in the “Chain of Custody” section of the DCIS Form 14.

18.7.b.(3).(a). If the ECS Custodian is the special agent responsible for obtaining or seizing the item, he/she will sign the “Released By” and the Alternate ECS Custodian will sign the “Received By” blocks in the “Chain of Custody” section of the DCIS Form 14 and reflect in the “Purpose” block that the item was released and received for **“Entry into the ECS.”**

18.7.b.(3).(b). If the Alternate ECS Custodian is the special agent responsible for obtaining or seizing the item, he/she will sign the “Released By” and the ECS Custodian will sign the “Received By” blocks in the “Chain of Custody” section of the DCIS Form 14 and reflect in the “Purpose” block that the item was released and received for **“Entry into the ECS.”**

18.7.b.(4). Enter the appropriate information into the Evidence Log in accordance with the procedures outlined in paragraph 18.6.b.(1). Ensure the Evidence Log number is placed in the “Log Number” block of the DCIS Form 14. Complete the DCIS Form 14 in accordance with the procedures set forth in paragraph 18.5.b.(2).

18.7.b.(5). If the submitted item was obtained from an ECS temporary storage container, ensure the original DCIS Form 14 submitted with the item is completed and remains with the ECS item. Place a carbon copy in the Active Custody File. Provide the remaining carbon copy for inclusion in the case file and a photocopy of the completed DCIS Form 14 to the releasing special agent.

18.7.b.(6). Ensure the original DCIS Form 14 is attached to the ECS item being stored.

18.7.b.(7). Ensure the ECS item is stored in accordance with the procedures outlined in sections 18.4. and/or 18.8.

(b)(7)(E)

18.9. Offsite Storage Procedures

18.9.a. As a general rule, all ECS items received by a DCIS Special Agent/office will be stored in an authorized ECS cabinet/ESA meeting the requirements of section 18.4. The items listed below, and other items as determined by the SAC that may need special and/or temporary storage, may be stored at an offsite facility as long as the integrity and accountability of the evidence is ensured for the duration of the storage and the storage procedures are in compliance with the procedures listed in this chapter:

(b)(7)(E)

18.9.b. With the prior authorization of the SAC, FO, or the designated supervisor, the types of materials mentioned above may be stored at an offsite facility where restricted physical access can be ensured. The following procedures apply to offsite temporary, as well as permanent, storage arrangements.

18.9.b.(1). All such items, unless of an especially bulky nature, will be wrapped or placed in containers and sealed with tamper-resistant tape so that any unauthorized access can be detected.

18.9.b.(2). When facility personnel will be maintaining temporary custody of the above types of material, they must be briefed on the requirement for secure storage and the potential requirement for them to testify as to their custody. They should be required to properly execute the original DCIS Form 14 upon receipt and release of the material.

18.9.b.(3). When the offsite facility is under DCIS control and the material is not to be released to facility personnel for temporary storage, the storage facility must meet the structural and security requirements of an ESA as outlined in section 18.4. Exemptions to these requirements must be approved by the SAC, FO.

18.9.b.(4). When a portion of the ECS item is stored at an offsite facility, a separate original DCIS Form 14 is required to accompany the item to the offsite facility. A copy of the DCIS Form 14 will remain in the Active Custody File. Upon receipt and release of the item, the offsite custodian will sign the original DCIS Form 14, as appropriate. When final disposition action occurs, return the original DCIS Form 14 to the ECS Custodian and place in the Final Disposition File.

18.9.c. The ECS Custodian is encouraged to conduct periodic liaison visits to local facilities to ensure that arrangements exist for the secure storage by DCIS of an ECS item that cannot be stored in a conventional FO/RA/PoD ECS storage cabinet/ESA. The location and contact point information should be placed in the Evidence Log and the contact point should be posted on the outside of the temporary storage facilities or in a convenient location within the FO/RA/PoD to assist DCIS personnel in storing such items without delay.

18.9.d. Items that meet the bulk/special handling storage requirements outlined in this section can be directly transferred from the location obtained or seized to the designated offsite storage facility.

18.9.d.(1). Upon determining the items obtained/seized are best suited for storage at the designated offsite storage facility, the seizing special agent will notify the ECS Custodian. If the ECS Custodian or Alternate is not available, the special agent should advise the cognizant SAC/ASAC or RAC of the intended destination of the items obtained/seized.

18.9.d.(2). An ECS item to be stored at an offsite storage facility under the control of a Military Criminal Investigative Organization (MCIO) or a Federal, state, or local law enforcement agency will be entered in its ECS. The obtaining/seizing special agent will ensure the DCIS Form 14 is complete and accurate prior to releasing items to the offsite storage facility personnel. The special agent and offsite facility representative will sign the appropriate "Released By" and "Received By" blocks on the DCIS Form 14. The original DCIS Form 14 will remain with the material being stored. A copy of the DCIS Form 14 will be expeditiously returned to the FO/RA/PoD ECS Custodian, who will keep a copy of the DCIS Form 14 in the Active Custody File with a notation as to the location of the ECS item.

18.9.d.(3). In the event the offsite storage facility is accessible to DCIS personnel only, the obtaining/seizing special agent will coordinate access with the ECS Custodian or the alternate to store and secure the material. The DCIS Form 14 and/or Evidence Tag will be affixed in accordance with the procedures in sections 18.5. and 18.7. A copy of the DCIS Form 14 will be provided promptly to the ECS Custodian, and arrangements will be made for the ECS Custodian to view the evidence prior to entry into the ECS. The original DCIS Form 14 will remain with the ECS item and a copy will be placed in the Active Custody File.

(b)(7)(E)

(b)(7)(E)

18.10. Inventory Procedures

18.10.a. When an item is first taken into custody by a DCIS Special Agent and determined to have evidentiary value in a potential prosecution, whether obtained or seized during the course of an investigation or received from another agency representative, the receiving special agent must complete a DCIS Form 14. The special agent may not rely on an inventory by the person from whom the item was received. Subsequently, when an item is transferred between special agents/agencies for any reason, the receiving special agent must again verify the inventory count unless it is received in a sealed condition. Such inventories should consist of an itemized count of each and every component. Once accomplished, every effort to package, seal, and appropriately mark the DCIS Form 15 should be accomplished by the special agent and the ECS Custodian to preclude the need for another itemized count.

18.10.b. Designated personnel perform inventories of the ECS for various reasons. Categories of inventories/inspections are listed below.

(b)(7)(E)

(b)(7)(E)

18.10.c. At a minimum, the inventory will always consist of a reconciliation of the Evidence Log against the Active Custody File and a visual accounting for each item(s) DCIS Form 15 to the DCIS Form 14 for which there is a log entry. An itemized count of each component is not necessary if the components have been appropriately sealed and tamper-resistant markings clearly reflect the component has not been molested.

18.10.c.(1). The only exception to the visual observation requirement will be an ECS item that, according to the Active Custody File, has been temporarily transferred to another activity.

18.10.c.(2). An ECS item stored outside the FO/RA/PoD because of its bulk, classification, or special nature will be reconciled during each inventory, as it is not considered to have been temporarily transferred.

(b)(7)(E)

18.10.d. When an inventory is completed, immediately enter in the Evidence Log the date of the inventory, the reason for the inventory, the names of those conducting the inventory, the results of the inventory, and the signatures of the participants. A similar entry will be made in the Evidence Log subsequent to any HQ-directed inspections.

18.10.e. List any discrepancy discovered during the course of an inventory by annotating the Evidence Log number and description of the item. Extensive information may be memorialized in a memorandum-for-record format and affixed to the Evidence Log for reference.

(b)(7)(E)

18.11. Quarterly Evidence Accounting. On a quarterly basis, HQ will request an accounting of all cash and all personal property valued in excess of \$2,500. This accounting is required by financial management regulations. Cash and monetary instruments maintained in DCIS ECS will be reported until transfer to the U.S. Marshals Service or final disposal. Personal property

maintained in DCIS ECS will be evaluated by whatever means is available, normally an Internet search, to determine the value for reporting. Personal property items determined to have a value in excess of \$2,500 will be included in this Quarterly Evidence Accounting (e.g., Rolex watches, critically acclaimed artwork, non-Government owned automobiles).

18.12. Transfer of Evidence

18.12.a. From time to time, a DCIS ECS item will need to be transferred from the DCIS office holding the item to an authorized recipient (e.g., an special agent with another agency, a prosecutor for use in court, a testing laboratory, or another DCIS office).

18.12.b. When it is necessary to transfer an ECS item to another agency on a temporary basis, the original DCIS Form 14 will usually accompany the ECS item. The chain of custody will be maintained in accordance with the following procedures.

18.12.b.(1). The ECS Custodian, prior to the release of the ECS item, will sign the original and a photocopy of the DCIS Form 14 in the “Released By” block and will note the reason for the transfer in the “Purpose” block. The original DCIS Form 14 will remain attached to the ECS item. Place the updated photocopy with original signature in the Active Custody File.

18.12.b.(2). Persons handling the ECS item prior to its return to the ECS Custodian will complete the appropriate “Received By” or “Released By” blocks on the accompanying original DCIS Form 14.

18.12.b.(3). Obtain a receipt from the receiving agency that provides for proprietary control of the evidence while it is not in the possession of DCIS. When registered mail or other commercial carrier (e.g., Federal Express) is used, the return receipt will suffice as a receipt. The tracking number will be annotated in the “Received By” block on all copies of the DCIS Form 14. In those instances when registered mail or commercial delivery is not used and the transfer is made by hand, make a photocopy of the updated original DCIS Form 14 and obtain an original signature from the person receiving the ECS item. Return the photocopy to the ECS Custodian to be placed in the Active Custody File.

18.12.b.(4). If only a portion of the ECS item is temporarily transferred, the ECS Custodian, prior to the release of the ECS item, will sign the original and a photocopy of the DCIS Form 14 in the “Released By” block and will note in the “Purpose” block the line item number that is being transferred. If only a portion of the items noted on a line is being transferred, the physical description of those items will be noted in the “Purpose” block. The reason for the transfer will also be noted in the “Purpose” block. The original DCIS Form 14 will accompany that portion of the ECS items being transferred. (Exception: the original DCIS Form 14 will remain with the portion of the ECS item that is needed for use in court.) Attach the updated photocopy with original signature to the balance of the ECS items maintained in the ECS. Place an updated photocopy of the original DCIS Form 14 in the Active Custody File. Upon return of the transferred item, the original DCIS Form 14 will replace the duplicate DCIS Form 14.

18.12.b.(5). Upon return of the transferred ECS items, the ECS Custodian will sign the “Received By” block only after inspecting each ECS item to ensure all ECS items are accounted for, itemized, and returned in their original condition. When a forensic laboratory has conducted destructive testing, the ECS Custodian will annotate the “Purpose” block to indicate that destruction has occurred. The notation will specifically describe the item returned and the condition of the item upon return.

18.12.c. When it is necessary to transfer an ECS item to another agency permanently, the original DCIS Form 14 will usually accompany the ECS item. The chain of custody will be maintained in accordance with the following procedures.

18.12.c.(1). The ECS Custodian, prior to the release of the ECS item, will sign the original and a photocopy of the DCIS Form 14 in the “Released By” block and will note the reason for the transfer in the “Purpose” block. The original DCIS Form 14 will remain attached to the ECS item. The updated photocopy with original signature will be placed in the Final Disposition File when disposition as noted in the “Final Disposition Action” section is confirmed.

18.12.c.(2). Obtain a receipt from the receiving agency that provides for proprietary control of the evidence while it is not in the possession of DCIS. When registered mail or other commercial delivery service is used, the tracking number and/or receipt will suffice as a receipt. Annotate the registered mail receipt or commercial shipper’s tracking number in the “Received By” block on all copies of the DCIS Form 14. In those instances when the transfer is made by hand, make a photocopy of the updated original DCIS Form 14 and obtain an original signature from the person receiving the ECS item. Return the photocopy to the ECS Custodian to place in the Final Disposition File.

18.12.c.(3). The agency representative receiving the ECS item will complete the “Final Disposition Action” section. Upon receipt of a copy of the completed “Final Disposition Action” section, the ECS Custodian will attach the photocopy in the Active Custody File to the completed “Final Disposition Action” section. Both will be placed in the Final Disposition File. The appropriate disposition entry will be made in the Evidence Log.

18.12.c.(4). If only a portion of the ECS items is being permanently transferred, annotate the original and two photocopies of the DCIS Form 14 as outlined in paragraph 18.12.b.(4).

18.12.c.(5). Obtain original signatures in the “Released By” and “Received By” blocks on the original as well as on both copies of the DCIS Form 14. In addition, the agency representative will receipt for that portion of the ECS items transferred by completing the photocopy of the “Final Disposition Action” section of one of the copies of the DCIS Form 14. A photocopy of the DCIS Form 14 will remain with the transferred evidence. The original DCIS Form 14 will be attached to the ECS item maintained by DCIS in the authorized cabinet/ESA. Place the remaining copy of the DCIS Form 14 with original signatures and the completed “Final Disposition Action” section in the Active Custody File.

18.12.c.(6). In the event the receiving agency declines to accept any part of the items identified for transfer, the receiving official will receipt for only those items accepted by making the appropriate notations on the DCIS Form 14. The original DCIS Form 14 bearing the receiving agency's original notations and receipt signatures, along with the item or items not accepted, will be returned to or by the ECS Custodian and placed in the appropriate authorized cabinet/ESA. Place a photocopy of the annotated original DCIS Form 14 in the Active Custody File.

18.12.c.(7). Final disposition of all ECS items listed on a DCIS Form 14 must occur **before** the DCIS Form 14 will be moved into the Final Disposition File and **before** the final disposition of the ECS item will be entered into the Evidence Log.

18.12.d. When it is necessary to transfer an ECS item from one DCIS office to another, the original DCIS Form 14 will usually accompany the ECS item. The chain of custody will be maintained in accordance with the following procedures.

18.12.d.(1). The procedures in paragraphs 18.12.b. and 18.12.c. will apply to the transfer of an ECS item from one DCIS office to another.

18.12.d.(2). When items are obtained or seized in response to a lead request, the special agent responding to the request, in coordination with the requesting special agent, will determine which items have evidentiary value. The special agent responding to the request will document items determined to have evidentiary value on a DCIS Form 14. Evidence obtained in response to a lead request may be transferred directly to the requesting office or may be entered into the ECS of the local office and stored pending transfer to the requesting office.

18.12.d.(3). The DCIS office requesting the ECS item will continue to use the DCIS Form 14 received from the transferring office. The ECS Custodian at the requesting office will place a carbon copy of the DCIS Form 14 in the Active Custody File and will give the other carbon copy of the DCIS Form 14 to the case agent to be placed in the case file.

18.12.d.(4). The ECS item 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 DCIS alphanumeric code and Evidence Log number assigned to the item by the originating office, e.g., 0035-94 (01DC-0126-92). The new number will be placed on the DCIS Form 14 above the original number.

18.12.d.(5). The office that transferred the ECS item, if all ECS items were in fact transferred, will remove its copy of the DCIS Form 14 from its Active Custody File, appropriately annotate the "Final Disposition Action" section, and place the document in the Final Disposition File.

18.12.e. The recipient of the ECS item is responsible for the security and condition of the item.

18.12.e.(1). The recipient is responsible for promptly reporting any damage or alteration to the item in his/her custody to the ECS Custodian.

(b)(7)(E)

18.13. Shipment of Evidence

(b)(7)(E)

18.13.d. When USPS registered mail is used, staple the registered mail receipt and the return receipt to the DCIS Form 14 maintained by the transferring office. When using Federal Express, United Parcel Service, or any other company with similar tracking capability, staple a copy of the shipping document indicating the tracking number to the DCIS Form 14 maintained by the transferring office. If the transfer is permanent, the receipts and/or shipping documents will become a permanent part of the ECS by inclusion in the Final Disposition File with the DCIS Form 14. If the material is subsequently returned to the office, the receipts and/or shipping documents may be destroyed upon final disposition of the ECS item.

18.13.e. All DCIS offices should instruct their mail and/or support personnel that when the presence of ECS material is apparent, the wrapping should not be disturbed and the package should be promptly delivered to the ECS Custodian. In no event should anyone other than the ECS Custodian open packages identifiable as ECS material.

18.14. Required Authority for Final Disposition Action

(b)(7)(E)

18.14.b. Obtain in writing approval for the final disposition of an ECS item used in a judicial, civil, or administrative process from the cognizant authority for disposition, usually the Assistant United States Attorney (AUSA) or legal counsel of the DoD Component affected by the investigation. Final disposition authority for an ECS item **not** used in a legal or administrative process will be obtained from the SAC/ASAC or designated supervisor.

18.14.b.(1). Do not dispose of an ECS item used in a judicial proceeding, either Federal, state, or other civilian court, until after the initial trial and subsequent appeals, if any, have been exhausted. Obtain authorization for disposition via letter to the prosecuting attorney involved in the original trial (Attachments F and G). If the original prosecutor is no longer available, obtain authorization from another prosecutor familiar with the case or from a supervisory prosecutor. Upon receipt of the written disposition authorization, the ECS Custodian will complete the "Final Disposition Action" section of the DCIS Form 14 by recording the name and title of the person authorizing the disposition and will attach the original disposition authorization to the DCIS Form 14. Proper disposition will then be made of the property.

18.14.b.(2). An ECS item used in an administrative process will not be released until all appeals or reviews of the initial action are completed. Obtain disposition authorization from the counsel or Judge Advocate who had jurisdiction over the person/company against whom the action was taken. In the event of their absence, contact their counterpart or a supervisor for disposition authorization. Upon receipt of the written disposition authorization, the ECS Custodian will complete the "Final Disposition Action" section of the DCIS Form 14 by recording the name and title of the person authorizing the disposition and will attach the original disposition authorization to the DCIS Form 14. Proper disposition will then be made of the property.

18.14.c. An ECS item considered pertinent to a DoD Component that may be disbanded or deactivated, or to an individual assigned to such a Component, will be returned to the requestor, subject, or victim when disposition authorization has been obtained in accordance with the procedures outlined in paragraphs 18.14.b.(1). and 18.14.b.(2). In those instances where, for either judicial or administrative purposes, DCIS must retain the item, the case agent should obtain the new location information for the command and/or individuals involved. Disposition authorization will be obtained from the AUSA, legal counsel of the gaining command, or the SAC/ASAC or designated supervisor, as appropriate.

18.14.d. Disposition authorization letters may be used to obtain the signature of cognizant authority for disposition. A photocopy of the DCIS Form 14 identifying the item to be

disposed of should be attached to the letter for reference purposes. If only a portion of the ECS items identified on the DCIS Form 14 are to be disposed of, the DCIS Form 14 and the letter should specifically identify those ECS items.

18.15. Disposition Procedures

(b)(7)(E)

18.15.a.(1). Property belonging to an individual, company, DoD Component, or another agency will, whenever possible, be returned to its rightful owner. An exception to this rule includes any property the mere possession of which is unlawful, e.g., controlled substances, illegal firearms, explosives, counterfeit U.S. or foreign obligations, or counterfeit identification.

18.15.a.(2). When an ECS item is to be returned to the owner or an authorized representative, the releasing and receiving individuals will sign the appropriate blocks of the DCIS Form 14.

18.15.a.(3). If the owner or a representative presents a DCIS Form 14 receipt copy when reclaiming property, the receipt copy should be destroyed. If the owner/representative is reluctant to destroy the receipt, both the owner/representative and the releasing party should annotate the receipt to show that the item was returned by noting the date of return and the condition of the item upon return.

18.15.a.(4). In the event that the owner refuses to accept all of the ECS items identified on the DCIS Form 14, or the owner cannot be identified or located after a reasonable effort, any item not returned will be disposed of in coordination with the Defense Reutilization and Marketing Office (DRMO).

18.15.a.(5). All U.S. Government property that cannot be identified as belonging to a particular activity or command will be submitted to the nearest DoD supply activity or DRMO for disposal. In addition to any documentation required by the receiving activity, the activity's representative should receipt for the property in accordance with the procedures outlined in section 18.12. In the event the activity declines to execute the DCIS Form 14, a suitable receipting document will be obtained and attached to the DCIS Form 14.

(b)(7)(E)

(b)(7)(E)

18.15.a.(8). Property that by its nature cannot be returned to the owner or entered into DoD supply channels or the DRMO for disposal, e.g., illegal firearms or other contraband, will be destroyed. In each instance, the SAC/ASAC or designated supervisor must authorize the destruction of the item, when necessary, after appropriate disposition authorization is obtained in accordance with section 18.14. Such destruction, with the exception of firearms, will be accomplished by or in the presence of the ECS Custodian and one other disinterested special agent or another trustworthy individual, both of whom will sign the “Final Disposition Action” section of the DCIS Form 14. (Note: Neither the SAC/ASAC, Evidence Custodian, Alternate Evidence Custodian, nor the designated ECS supervisor will act as a witness to the destruction of an ECS item.) Such destruction will be of a nature so as to make the item unusable for any lawful or unlawful purpose other than residual scrap.

18.15.b. Dispose of firearms by returning the weapon to the legal owner or transferring the weapon to the appropriate local office of the Bureau of Alcohol, Tobacco, and Firearms (BATF).

18.15.b.(1). Firearms belonging to an individual or company will be returned only when ownership can be verified and possession is legal. The owner or designated representative will receipt for the firearm by signing the DCIS Form 14 in the appropriate block. In the event other ECS items identified on the DCIS Form 14 are to remain in the ECS, the original DCIS Form 14 will be maintained with the remaining ECS items and an updated copy will be placed in the Active Custody File. If the firearm is the only item inventoried on the DCIS Form 14, the original DCIS Form 14 will be placed in the Final Disposition File. In either case, annotate the Evidence Log to reflect the release of the firearm.

18.15.b.(2). Government-owned firearms being returned to a DoD Component or other agency from which the firearm was obtained, seized, or stolen will be transferred in accordance with the procedures outlined in section 18.14. In the event the probability exists that a weapon is Government-owned, but the identity of the DoD Component or other Government agency from which the weapon was stolen cannot be determined, the ECS Custodian will coordinate the transfer/destruction with the appropriate local BATF office. No DCIS office may accept permanent custody of such weapons without the approval of the AIGI-INV, nor may a DCIS office dispose of any firearm that has been permanently transferred to DCIS custody without receiving the approval of the AIGI-INV.

18.15.c. Dispose of the recordings of consensual and nonconsensual interceptions in accordance with SAM Chapter 42, “Investigative Records Management.”

(b)(7)(E)

18.16. Laboratory Examination of Evidentiary Material

18.16.a. DCIS special agents are encouraged to use crime laboratories when appropriate. Laboratory support is available from a number of Federal, state, and local agencies offering a full range of forensic examinations of evidentiary material. Among those agencies supporting DCIS are the U.S. Army Criminal Investigation Laboratory, FBI, U.S. Postal Service, BATF, and numerous state and local law enforcement laboratories. Additionally, the Defense Logistics Agency has an approved certified mechanical laboratory and has compiled a list of contracted laboratories and their capabilities. Transfer ECS material for examination purposes in accordance with the procedures outlined in section 18.12.

18.16.b. When a laboratory examination is required, the requesting special agent will ensure that laboratory personnel involved are court certified in their respective area of expertise.

ATTACHMENTS

<u>Attachment</u>	<u>Title</u>
A	DCIS Form 15, Evidence Tag (May 1985)
B	DCIS Form 14/14(A), Defense Criminal Investigative Service Evidence Custody Document (Jan 2011)
C	Sample Evidence Log Captions
D	DCIS Form 14, Defense Criminal Investigative Service Evidence Property Receipt (Nov 1996)
E	Seized Cash Deposit Instructions
F	Disposal Authorization Letter with Attachment (subpoenaed)
G	Disposal Authorization Letter with Attachment (seized)

ATTACHMENT A

DCIS FORM 15, EVIDENCE TAG

DCIS EVIDENCE TAG			
ITEM NO.	LOG NUMBER		NAME OF SUBMITTING AGENT
DESCRIPTION OF ARTICLE <i>(Include quantity)</i>			
NAME OF PERSON FROM WHOM PROPERTY SEIZED			

DCIS Form 15 (May 85) ☆ GPO:1991-295-294

(Tie-on Tag)

DCIS EVIDENCE TAG			
ITEM NO.	LOG NUMBER		NAME OF SUBMITTING AGENT
DESCRIPTION OF ARTICLE <i>(Include quantity)</i>			
NAME OF PERSON FROM WHOM PROPERTY SEIZED			

DCIS Form 15 (May 85) ☆ GPO:1991-295-293

(Stick-on Tag)

ATTACHMENT B

DEENSE CRIMINAL INVESTIGATIVE SERVICE EVIDENCE CUSTODY DOCUMENT

OFFICE	CASE CONTROL NUMBER	LOG NUMBER	DATE AND TIME OF SEIZURE	
NAME OF PERSON FROM WHOM PROPERTY SEIZED		LOCATION WHERE PROPERTY SEIZED		
CASE TITLE				
ITEM	QUANTITY	DISPOSITION ACTION	DESCRIPTION OF PROPERTY - MODEL NUMBER, SERIAL NUMBER, IDENTIFYING MARKS, CONDITION, AND VALUE WHEN APPROPRIATE	
NAME AND SIGNATURE OF WITNESS (IF AVAILABLE)		NAME AND SIGNATURE OF RECEIVING S/A		
CHAIN OF CUSTODY				
ITEM	DATE & TIME	RELEASED BY	RECEIVED BY	PURPOSE
		NAME	NAME	
		ORGANIZATION	ORGANIZATION	
		SIGNATURE	SIGNATURE	
		NAME	NAME	
		ORGANIZATION	ORGANIZATION	
		SIGNATURE	SIGNATURE	

CHAIN OF CUSTODY (Continued)

ITEM	DATE & TIME	RELEASED BY	RECEIVED BY	PURPOSE
		NAME	NAME	
		ORGANIZATION	ORGANIZATION	
		SIGNATURE	SIGNATURE	
		NAME	NAME	
		ORGANIZATION	ORGANIZATION	
		SIGNATURE	SIGNATURE	
		NAME	NAME	
		ORGANIZATION	ORGANIZATION	
		SIGNATURE	SIGNATURE	

REMARKS

FINAL DISPOSITION ACTION

FINAL DISPOSITION AUTHORITY

NAME (PRINTED)
RANK/TITLE
ORGANIZATION

PERSON(S) RECEIVING ITEM(S)/WITNESSING DESTRUCTION

NAME

ORGANIZATION

SIGNATURE/DATE

MAY BE CONTINUED IN REMARKS IF NECESSARY

INDICATE IN DISPOSITION ACTION COLUMN (ON FRONT) BY NUMBER AND LETTER CODE PERSON(S) RECEIVING OR WITNESSING ACTION AND TYPE OF ACTION. RETURNED TO INDIVIDUAL OWNER (I), RETURNED TO COMMAND (C), TURNED INTO SUPPLY (S), TO ANOTHER AGENCY (A), DESTROYED (D),

DEFENSE CRIMINAL INVESTIGATIVE SERVICE EVIDENCE CUSTODY DOCUMENT

18-B-2

May 2011

CHAIN OF CUSTODY CONTINUATION SHEET

OFFICE		CASE CONTROL NUMBER	LOG NUMBER	REMARKS
ITEM	DATE & TIME	RELEASED BY	RECEIVED BY	PURPOSE
		NAME	NAME	
		ORGANIZATION	ORGANIZATION	
		SIGNATURE	SIGNATURE	
		NAME	NAME	
		ORGANIZATION	ORGANIZATION	
		SIGNATURE	SIGNATURE	
		NAME	NAME	
		ORGANIZATION	ORGANIZATION	
		SIGNATURE	SIGNATURE	
		NAME	NAME	
		ORGANIZATION	ORGANIZATION	
		SIGNATURE	SIGNATURE	
		NAME	NAME	
		ORGANIZATION	ORGANIZATION	
		SIGNATURE	SIGNATURE	
		NAME	NAME	
		ORGANIZATION	ORGANIZATION	
		SIGNATURE	SIGNATURE	

DCIS Form 14(A)

□

ATTACHMENT C

SAMPLE EVIDENCE LOG CAPTIONS

LOG NUMBER DATE RECEIVED	CCN NO.	BRIEF DESCRIPTION OF EVIDENCE	FINAL DISP DATE	FINAL DISP.	REMARKS
0098-92 3/1/92	9010004N	F-14 Engine Housing Unit	7/8/94	Return to Air Force	None

ATTACHMENT D

DEFENSE CRIMINAL INVESTIGATIVE SERVICE EVIDENCE PROPERTY RECEIPT

OFFICE	CASE CONTROL NUMBER	LOG NUMBER	DATE AND TIME OF SEIZURE
NAME OF PERSON FROM WHOM PROPERTY SEIZED		THIS RECEIPT MUST BE PRESENTED TO OBTAIN RELEASE (IF APPROPRIATE) OF ITEM(S) LISTED BELOW.	
The property listed below was received this date by a Special Agent, Defense Criminal Investigative Service			
ITEM	QUANTITY	DESCRIPTION OF PROPERTY - MODEL NUMBER, SERIAL NUMBER, IDENTIFYING MARKS, CONDITION, AND VALUE WHEN APPROPRIATE	
NAME AND SIGNATURE OF WITNESS (IF AVAILABLE)		NAME AND SIGNATURE OF RECEIVING S/A	

DCIS Form 14 (Nov.96)

CHAPTER 19

SEARCHES

<u>Contents</u>	<u>Section</u>
General	19.1.
Searches Under Search Warrant	19.2.
Search Incidental to Arrest	19.3.
Search by Consent	19.4.
Emergency Searches	19.5.
Command-Authorized Searches	19.6.
Abandoned Property	19.7.
Search of Vehicles	19.8.
Marking Evidence for Identification	19.9.
Diplomatic Immunity	19.10.
Choice of Search or Less Intrusive Means	19.11.

19.1. General. Fourth Amendment provisions of the Constitution require that searches of persons or premises and the seizure of evidence or contraband articles be reasonable. The test of reasonableness is met by the existence of facts and circumstances which, when reviewed by an approving authority, provide that authority with probable cause to believe that evidentiary or contraband articles are located at the place or on the person to be searched. The Constitution contains specific prohibitions against unreasonable search and seizure. The Constitution also safeguards an individual's privacy under circumstances in which an expectation of privacy is reasonable. This protection includes an individual's person, property, residence, vehicle, conversations, private papers, and records.

19.2. Searches Under Search Warrant

19.2.a. **Policy.** It is DCIS policy, in accordance with Title 10, United States Code (U.S.C.), §1585a, to always obtain a search warrant from a Federal magistrate or state court of record prior to initiating a search. Before conducting a search of persons or premises in which evidence or contraband items are likely to be found, DCIS Special Agents will obtain a warrant in the manner described in Rule 41, Federal Rules of Criminal Procedure (FRCP). This policy is subject to the following exceptions:

- 19.2.a.(1). search incident to arrest,
- 19.2.a.(2). search by consent,
- 19.2.a.(3). search under emergency or exigent circumstances.

NOTE: Before contacting a Federal Magistrate or state court of record for the specific purpose of making an application for a search warrant, obtain the concurrence of an Assistant United States Attorney (AUSA) located in the judicial district in which the warrant is to be served. Request that the AUSA review the affidavit of probable cause for legal sufficiency before obtaining the warrant. Retain copies of the approved affidavit and search warrant obtained from the Federal magistrate or state court of record in the appropriate DCIS case file.

(b)(7)(E)

(b)(7)(E)

19.2.1. Leaving Warrant and Receipt. During the execution of a search warrant, special agents are required to give a copy of the warrant to the individual whose person, premises, or property is searched. The fact that evidence or contraband is not seized does not excuse special agents from providing the required copy of the warrant to the individual involved. In addition, give a receipt for any money, documents, or other property seized, whether under authority of the warrant or otherwise. Thus, items seized in plain view or a weapon taken for safety reasons, though not described in the warrant, should be included in the receipt. The receipt is to be in the form of an itemized list of all property taken. Ensure that the description of all items is adequate and accurate. Prepare the receipt in triplicate. The original will accompany the warrant upon return to the Federal magistrate or state court of record where the warrant was issued. Give the second copy to the person searched. Retain the third copy in the case file. At the conclusion of the receipt, affix the following certificate and attempt to obtain the signature of the person from whose possession the property was taken. Two special agents, or one special agent and another person should witness this certificate (see example at Attachment B). If the person whose premises was searched declines to sign such a statement, it should be so noted, witnessed, and signed by the special agents and a copy left at the search site. If the person from

whose possession evidence is seized is not present, leave a copy of the warrant and the receipt in a conspicuous place at the location of the search. When special agents executing the search warrant do not seize property, obtain a certificate, signed and witnessed as indicated (see example at Attachment C).

19.2.m. **Return.** On the reverse side of a search warrant is a format used to return the warrant to the Federal magistrate or state court of record where the warrant was issued. The return serves as a report to the magistrate or court that the warrant was executed as directed. The return will be made as soon as possible following the execution of the warrant. The return also requires a written inventory of property taken pursuant to the warrant. The written inventory must accompany the warrant when returned to the Federal magistrate or state court of record. The inventory consists of an accurate itemized list of items seized. To the extent possible, the inventory should be made in the presence of the special agent making application for the warrant and the person from whom the property was taken. If the person from whom the property was taken is not present, the inventory will be made in the presence of at least one credible person other than the special agent making application for the warrant. The special agent making the original application for the warrant will verify the inventory prior to making the required return. In his/her absence, another special agent conducting the search will verify the required inventory, and submit the inventory to the special agent making the application for the warrant prior to the final return being made.

19.2.n. **Damage to Property.** Forcible entry to execute an authorized search may result in a property owner's entitlement to compensation for doors and/or windows damaged due to the required entry. Government funds are available for satisfaction of justified claims arising from such damage. In a case where a claim is likely to be filed, the special agent conducting the search will ensure that photographs/videos of the damage are obtained and that the details surrounding the damage are recorded in a memorandum for record.

19.2.o. **Securing the Premises.** Special agents serving search warrants are required to ensure that premises searched are secured at the conclusion of the search. In the absence of an occupant, take whatever steps are necessary to render the premises inaccessible to neighbors, vandals, etc. In situations involving forced entry, broken doors and windows will be replaced, repaired, or boarded up before special agents depart the premises. If a third party such as a carpenter is required to secure the premises, a special agent will remain until such work is completed. To the extent possible, premises disrupted by the search will be restored to their original condition. Special agents conducting the search may elect to photograph/video the interior and exterior of the premises prior to departing in order to protect participating special agents against allegations of impropriety or illegality. However, when it is anticipated that later claims of harassment will be made by those affected by the search, photographs/video of the interior and exterior are required.

19.2.p. **Criminal Liability.** All DCIS Special Agents should be thoroughly familiar with 18 U.S.C. §§2234, 2235, and 2236. These sections address criminal liability associated with inappropriate actions and misuse of the Federal search warrant process. Specifically, a special agent who, in executing a search warrant, willfully exceeds authority or exercises authority with unnecessary severity may be guilty of a criminal offense under 18 U.S.C. §2234.

A special agent who maliciously and without probable cause procures a search warrant and causes the warrant to be issued and executed may be found guilty of a criminal offense under 18 U.S.C. §2235. Special agents can be held criminally liable if they search any private dwelling without a warrant, or maliciously and without reasonable cause search any building or property without a warrant in violation of 18 U.S.C. §2236.

19.2.q. **Recovery of Money.** Whenever money or other property consisting of numerous items requiring counting is obtained in connection with a DCIS investigation, two special agents will independently count the money or property and their results compared for the purpose of verifying the accuracy of the count and detecting any errors.

19.2.r. **Weapons and Serial Numbered Items.** Whenever weapons are seized as a result of a search, they shall be checked through the National Crime Information Center (NCIC) to determine whether they have been reported stolen, lost, or missing, or are wanted in connection with the commission of a crime. All other serial numbered items seized during a search should also normally be checked through NCIC.

19.2.s. **Debriefing.** After all operational matters have been completed in regard to the service of a search warrant, the senior case agent shall schedule a debriefing. The debriefing should take place as soon as possible after the service of the warrant, and attendance of all participants should be encouraged. Address items such as the level of participation by outside agencies and “lessons learned” at the debriefing. Participants should bring to the attention of the case agent any items or incidents that may arise at a later date as a result of the search.

19.3. Search Incidental to Arrest

19.3.a. **Policy.** DCIS Special Agents have statutory arrest authority pursuant to 10 U.S.C. §1585(a). Any DCIS Special Agent conducting an investigation within DCIS jurisdiction may apprehend persons subject to the Uniform Code of Military Justice upon reasonable belief that an offense has been committed and that the person is the offender.

19.3.b. **Right to Search.** The authority to search a person following a full custody arrest is an exception to Federal search warrant requirements. The exception arises when an authorized special agent makes a full custodial arrest with the intent of taking the arrested person to jail or before a magistrate to be dealt with according to the law. The nature of the crime, whether a felony or a misdemeanor, has no bearing on the right to search. The imposition of physical custody is the key to any such search. A full and complete search of the person arrested may be made for evidence connected with the crime for which the person has been arrested. Additionally, the person arrested may be searched for weapons or implements of escape. The purpose of the immediate search is to protect arresting special agents, to prevent escape, and to preserve any evidence in the custody of the person arrested. Any search incidental to arrest shall be made by two or more special agents, one as the search agent and one as cover agent.

19.3.c. **Need for Lawful Arrest.** If an arrest is made without probable cause or is made without a warrant and no warrant exception exists, the arrest is invalid. Any incidental search is

also invalid, and any evidence uncovered may be subject to exclusion. The best assurance that the arrest and incidental search will be upheld if later challenged by the defense is to obtain an arrest warrant before imposing custody.

19.3.d. **Good Faith Arrest.** An arrest, although lawful, may not be used as a pretext to search for evidence of a different and unrelated crime. The arrest and subsequent search must be in good faith. When an arrest is made in good faith, evidence of an unrelated crime discovered inadvertently in the course of a search incident to the arrest will remain admissible.

19.3.e. **Contemporaneous Search.** Special agents imposing custody should generally make the search of a person incidental to an arrest at the time and place of arrest. A search of the area immediately surrounding or in the control of the person arrested should be conducted at the time of or shortly after the arrest while the person in custody is still present. A more thorough search of an arrested person is justified as incidental to the arrest after the person arrested has been transported to another location (e.g., at the time the arrested person is incarcerated in jail).

(b)(7)(E)

(b)(7)(E)

19.3.i. Inventory of Personal Property. Special agents should carefully inventory items of personal property prior to being stored for safekeeping that have been removed from an arrested person prior to incarceration. Prepare a receipt for such property and give the receipt to the person arrested. The inventory should include the contents of containers such as purses, shoulder bags, suitcases, briefcases, etc. In the event that personal containers are locked or sealed, great care should be taken to minimize damage to the container or the contents while gaining access. This caretaking function must not be construed as an alternative to a search warrant whenever there is probable cause to believe that evidence or contraband is inside a container. Under those circumstances, the container should be secured until a search warrant can be obtained.

(NOTE: Generally, the law has been that a search of a container cannot be justified as incidental to arrest if the search is remote in time and place from the arrest. The inventory of containers (locked or unlocked) is allowed at a police station after a suspect has been arrested. In instances involving locked containers, special agents should consult with an AUSA within the jurisdiction of the search.)

(b)(7)(E)

19.3.k. **Receipt and Certificate.** Give a receipt for any property taken in a search incidental to arrest to the person from whom the property is taken. The receipt is an itemized list describing each item seized. Prepare the receipt in duplicate. Give a copy to the person from whom the property was obtained. Retain the original receipt in the case file. Have the person from whom the property was taken initial erasures or corrections on the receipt. The receipt must contain a certificate acknowledging the search and seizure of property and is to be signed by the person from whom the property was taken. A special agent conducting the search will witness the receipt. The format for the certificate described is found in paragraph 19.2.l. (see example at Attachment B). When no evidence is seized, obtain a certificate to that effect (see example at Attachment C). If the person from whom the property was seized refuses to sign a receipt, it should be so noted and witnessed.

19.4. Search by Consent

19.4.a. **Exception to Search Warrant.** A search made with the voluntary consent of one authorized to give consent is lawful as an exception to the search warrant requirement. A consent is a relinquishment of Fourth Amendment rights by the consenting party, and thus a consensual search is reasonable even in the absence of probable cause.

19.4.b. **Lawful Possession.** Special agents seeking permission to search without a warrant must obtain consent from a person authorized to give it. Only a person legally in possession and control of the concerned property or premises, to the exclusion of others, may give consent. As in the case of landlord and tenant or innkeeper and guest, ownership is not the equivalent of lawful possession when the owner has temporarily yielded his or her right to possess. Additionally, lawful presence is not the same as lawful possession. A guest lawfully on the premises is generally not authorized to give up rights possessed by his or her host. Special agents should make certain that consent is obtained from one in authority. Any doubt as to who possesses the premises or property should be resolved before proceeding. Carefully question any person present who might be of help in deciding who is authorized to consent.

19.4.c. Joint Possession

19.4.c.(1). When two or more persons jointly possess the concerned property or premises, any of the individuals may consent to a search. Joint possessors assume the risk of disclosure when they agree to share the property. However, places or items of personal property reserved for the exclusive use of one person may not be searched by consent of another. For example, the joint tenant in an apartment may consent to a search of all commonly possessed areas within the premises (e.g., the bathroom, kitchen, linen closet, and china cabinet), but may not consent to the search of a bedroom or closet or briefcase possessed exclusively by the other tenant. A consent search should not be undertaken when joint possessors are present and one objects to the search. Rules relating to joint possession apply in a wide variety of relationships (e.g., husband and wife, cohabitants, business partners, confederates in crime).

19.4.c.(2). As a general rule, parents may consent to the search of a family dwelling directed against children residing therein and being supported by the parents. On the

other hand, since Fourth Amendment protection belongs to the parents, children may not relinquish the parents' rights by consenting to a search of the family home directed against them.

19.4.c.(3). An employer may be barred from permitting a search of personal property reserved for the exclusive use of an employee. By terms of an employment contract, an understanding of the parties, or by accepted custom and practice, employees might acquire a reasonable expectation of privacy in their desks, lockers, or toolboxes. An employer would not be empowered to permit a search of the personal property reserved for the employee's exclusive use.

19.4.c.(4). The capacity of an employee to permit the search of business premises depends upon the authority given by the employer or principal. A special agent seeking consent to search business premises in the absence of the resident manager should obtain consent from the highest-ranking official available. While a search warrant is preferred, business records may be searched by consent. Obtain such consent from the custodian of records or official in charge.

19.4.d. **Voluntariness.** The critical issue in any consent search is whether the consent is voluntary. The consent to search must be the result of a free and unconstrained choice. It is the Government's burden to prove the consent was not coerced. Special agents should avoid any actions or statements likely to elicit submission as a result of their authority rather than a free choice. No single criterion can be used to determine voluntariness. Consider the number of special agents present, the time of the search, the manner of the request, promises made or implied to induce consent to search, the display of weapons, and the physical or mental condition of the consenter. Formal custody alone will not invalidate a consent. A person under arrest may give permission to search his/her house, vehicle, or other property. However, special agents should be cognizant of the fact that custody is an important factor used to consider voluntariness. A prosecutor's burden of showing voluntary consent is heavier in instances where the subject has been taken into custody prior to giving consent. Using physical force, threats, fraud, deceit, or misrepresentation will taint the consent and render the consent involuntary. A consent to enter obtained during the course of an undercover operation is considered to be proper.

19.4.e. **Warning of Rights.** The Government is not required to prove that a warning relating to Fourth Amendment rights was administered prior to obtaining a voluntary consent to search. However, since Fourth Amendment rights are a factor bearing on voluntary consent, inform individuals from whom consent is requested that they have a right to withhold consent.

19.4.f. **Proof of Consent.** If possible, obtain in writing a consent to search. Use DCIS Form 33, Permissive Authorization for Search and Seizure (Attachment D) for this purpose. In the event that an individual orally consents to a search but declines to sign the form, the special agent receiving the consent will make a record of the individual's consent on DCIS Form 33, which should be witnessed by another special agent. Complete the form except for the signature of the consenting party. Record on the DCIS Form 33 the circumstances and facts relating to the consent, preferably in the language of the consenter. Retain the completed DCIS Form 33 in the case file.

19.4.g. **Limitations on Consent.** The consenting party controls the conditions of a search. He/she may revoke the consent, at which time special agents should terminate the search; or he/she may otherwise limit the scope or time of search. Special agents must conform to such limitations.

19.4.h. **Implied Consent.** The failure of a subject to object, or the fact that the subject remains silent, cannot be considered voluntary consent. Special agents should not consider a subject's failure to object, silence, or any other ambiguous response as a relinquishment of Fourth Amendment rights. To the extent possible, obtain an express consent in writing. In the absence of a written consent, obtain a specific verbal consent witnessed by members of the search team.

19.4.i. **Receipt and Certificate.** Prepare and give a receipt to the consenting party for any property seized during a consent search. The receipt is to be in the form of an itemized list that accurately describes all property taken. Prepare the receipt in duplicate. Retain the original for the case file, and give a copy to the consenter. At the conclusion of the search, a certificate acknowledging the search is to be signed by the consenting party and witnessed by the searching special agents. The format for the certificate is the same as that described in paragraph 19.2.i. (see example at Attachment B). Where no evidence is seized as a result of the search, obtain a certificate to that effect from the consenting party (see example at Attachment C).

(b)(7)(E)

19.6. Command-Authorized Searches. The authority to approve this type of search resides in the commander, and it is up to the commander to decide to whom authorization is given to conduct the search. The same regulations and authority as the Military Criminal Investigative Organizations guide DCIS. Command-authorized searches can be used on military installations or areas under military control. Before a search is conducted, determine whether a command-authorized search or a search warrant should be used. The decision should always be discussed with the appropriate AUSA.

19.7. Abandoned Property

19.7.a. Abandonment of premises or property, both real and personal, relieves the former possessor of the right to assert that his or her Fourth Amendment rights were violated.

Therefore, special agents may enter, search, and/or seize abandoned premises and property without first obtaining a search warrant. Unlike most areas of search and seizure, the courts are not concerned with the existence of any probable cause at the time of a search or seizure based on abandonment. Abandoned property has no Fourth Amendment protection because either (1) the defendant has given up a reasonable expectation of privacy in that property, or (2) the defendant no longer has standing to object to use of the evidence in court, or (3) both. The search of the property is justified based solely on the fact that the property or the individual's privacy interest in that property is deemed abandoned. As long as the court finds that the property was abandoned prior to the search or seizure by a special agent, then the actions of the special agent will be legal whether or not the special agent knew that the property was in fact abandoned at the time of seizure. Because of the difficulty in proving abandonment, special agents should enter and search abandoned premises and property only when it is impractical to obtain a search warrant or when they have discussed the situation with and received concurrence from the cognizant prosecutor.

19.7.b. If property is discarded in a traditionally private area, e.g., an individual's home or on the curtilage, it is not considered to be abandoned per se. Some other actions will be required to show not only the act of discarding or abandoning, but also the actual intent to relinquish the expectation of privacy. An example of this is where an individual discards items in his trashcan in his dwelling or on his curtilage. The item normally would not be considered abandoned until it is removed from the curtilage for garbage pickup or until the garbage collectors have taken possession of the property.

19.8. Search of Vehicles

19.8.a. **Authority.** The same authority that allows searches of persons and premises applies to motor vehicles. A search warrant may be used to search a vehicle located in the jurisdiction where the warrant is outstanding. It may also be searched by the consent of a party having lawful possession of the vehicle. Vehicles may also be searched without a warrant if the search is made pursuant to the arrest of a driver or an occupant and the arrest occurs within or in close proximity to the vehicle. The general rule that a search incident to arrest may extend to those areas within the immediate control of the person arrested at the time of the arrest has been constructed to mean the entire passenger compartment, to include luggage, boxes, bags, clothing, and an open or closed glove compartment and consoles.

(b)(7)(E)

(b)(7)(E)

19.8.b. **Vehicle Exception.** The most common form of exigent circumstances is when a conveyance that special agents have probable cause to believe is carrying items subject to seizure (contraband, means and instruments of a crime, etc.) is found moving about on the highways, waterways, etc. Conveyances include automobiles, trucks, airplanes, boats, and common carriers. In such a situation, seeking a search warrant is not practical prior to stopping and searching the conveyance. By the time a warrant could be obtained, the conveyance and its suspected evidentiary cargo could be hidden, destroyed, or removed from the court's jurisdiction.

This exception to the search warrant requirement is called the “mobility doctrine” or the “Carroll Doctrine” after the case of *Carroll v. United States* (267 U.S. 132 (1925)) in which the Supreme Court first recognized the exception. The “automobile exception” to the Fourth Amendment’s warrant requirement established in *Carroll* applies to searches of vehicles that are supported by probable cause to believe that the vehicle contains evidence of a crime. Once the requirements for a *Carroll*-type search have been met, a warrantless search may be made that is as thorough as a magistrate judge could authorize by a warrant. When law enforcement agents have probable cause to search a vehicle, they may conduct a warrantless search of every part of the vehicle, including all containers and packages that may conceal the object of the search. The scope of the search is not defined by the nature of the container in which the evidence is secreted; rather, it is defined by the object of the search and the places in which there is probable cause to believe that it may be found.

19.9. Marking Evidence for Identification. All articles legally seized as evidence or contraband should be carefully marked or labeled for identification. Identification marks should not damage the evidence. Marks should be made in such a manner as to preclude the possibility of the marks being obliterated. The identification marks should be distinctive in order to make it possible for the special agent who collected the evidence to testify at a later date that this particular article was found at a certain place at a certain time. Evidence obtained and placed in containers or cellophane envelopes should be appropriately identified or labeled. Detailed notes should be made describing (1) the article found; (2) the time, date, and place the article was found; (3) the person who found the article; and (4) the identifying mark on the article. If the evidence contains serial numbers or other identifying numbers (e.g., guns, computers, typewriters), the special agent finding the evidence should record those numbers. The special agent should preserve original notes in the investigative file for use if called upon to testify in court. SAM Chapter 18, section 18.7, details specific instructions on entering articles obtained via a search into the DCIS Evidence Custody System (ECS), once review and analysis has determined the item of evidentiary value to the investigation. Prior to entry into the ECS, articles and items obtained via a search should be clearly identified, segregated, and safeguarded from other articles and items, until such time a thorough review and analysis for evidentiary value to the investigation is accomplished.

19.10. Diplomatic Immunity. Diplomatic representatives of foreign governments in the United States are exempt from arrest by all Federal or state officers. Special agents may not enter offices or dwellings of representatives possessing diplomatic immunity for the purpose of making a search or seizure. In the event an individual identifies himself as a diplomat or the place to be searched is a diplomatic mission, special agents will contact Headquarters immediately for verification and additional instructions.

19.11. Choice of Search or Less Intrusive Means. In choosing whether to use the search warrant process, or an alternate and less intrusive means (e.g., subpoenas) to obtain documents, special agents should consider:

19.11.a. whether use of the alternate means will give advance notice of the Government’s interest, with the resulting likelihood of destruction, alteration, or concealment of the documents or other potential evidence;

19.11.b. whether the Government has an immediate need to obtain the documentary materials;

19.11.c. whether the items to be seized can be identified by the special agent (relevant records as distinguished from irrelevant records).

ATTACHMENTS

<u>Attachment</u>	<u>Title</u>
A	Sample Tactical Operations Plan
B	Example of Certificate Statement When Property Is Taken
C	Example of Certificate Statement When Property Is NOT Taken
D	DCIS Form 33, Permissive Authorization for Search and Seizure

CHAPTER 20

ARRESTS

<u>Contents</u>	<u>Section</u>
General	20.1.
Policy	20.2.
Training Requirements	20.3.
Use of Force	20.4.
Execution of Arrest Warrants	20.5.
Non-Federal Crimes	20.6.

20.1. General

20.1.a. This chapter provides background, policy, and procedures for making arrests with or without a warrant. These policies and procedures are in accordance with the following references.

20.1.a.(1). Title 10, United States Code (U.S.C.), section 1585a, Special Agents of the Defense Criminal Investigative Service: authority to execute warrants and make arrests.

20.1.a.(2). Federal Rules of Criminal Procedure, Rule 3, The Complaint; Rule 4, Arrest Warrant or Summons on a Complaint; Rule 5, Initial Appearance; and Rule 9, Arrest Warrant or Summons on an Indictment or Information.

20.1.a.(3). Manual for Courts Martial, United States, Chapter III, Rule 302, Apprehension.

20.1.a.(4). Defense Criminal Investigative Service (DCIS) Special Agents Manual (SAM), Chapter 1, “Organization, Mission, Jurisdiction, and Authorities,” paragraph 1.5.d., “Arrest Authority.”

20.1.a.(5). Department of Defense Instruction 5505.14, “DNA Collection Requirements for Criminal Investigations,” May 27, 2010.

20.1.a.(6). U.S. Attorney General Memorandum, “DNA Sample Collection from Federal Arrestees and Defendants,” undated.

20.1.b. The execution of an arrest warrant is potentially dangerous since people react in unpredictable ways when arrested. Every DCIS Special Agent who manages, supervises, or assists in the execution of an arrest warrant should be mentally and physically prepared for any situation. Careful planning can eliminate some risks and reduce others. Caution, common sense, good judgment, and preparation are essential for the safe execution of an arrest. A sample Tactical Operations Plan is available on the intranet on the DCIS Special Agents Toolbox.

20.2. Policy. When the need to make an arrest is reasonably foreseeable, a warrant shall be obtained and the arrest shall be made in accordance with the above references and this chapter. Warrantless arrests should be made only under exigent circumstances.

20.3. Training Requirements. Prior to being authorized to make arrests, a DCIS Special Agent must have completed the following training.

20.3.a. The Criminal Investigative Training Program at the Federal Law Enforcement Training Center (FLETC), Glynco, GA, or the equivalent Federal criminal investigative training such as that provided by the Federal Bureau of Investigation (FBI). The Special Agent in Charge, Internal Operations Directorate, in coordination with the Special Agent in Charge of the field office, will make the determination as to the acceptability of the Federal training.

20.3.b. Use of Force training and be authorized to carry firearms in accordance with SAM Chapter 38, "Use of Force."

20.4. Use of Force A DCIS Special Agent will comply with all requirements of SAM Chapter 38, "Use of Force," to lawfully control an individual, during an arrest situation, or to accomplish the law enforcement purpose for which the arrest is justified.

20.5. Execution of Arrest Warrants

20.5.a. Supervisory Responsibilities

20.5.a.(1). Upon request of a subordinate special agent, discuss and approve, if appropriate, the request to seek an arrest warrant. Determine whether the DoD nexus and probable cause exist and, if so, authorize the special agent to seek a warrant.

20.5.a.(2). Ensure the execution of every arrest warrant is coordinated with the appropriate prosecutor and that it is carefully planned, particularly with regard to the safety of special agents, subjects, and uninvolved parties.

20.5.b. Special Agent Responsibilities

20.5.b.(1). When the facts of an investigation support a finding of probable cause, special agents will coordinate the specifics with their immediate supervisor and gain approval to obtain an arrest warrant.

20.5.b.(2). Special agents should make arrests without warrants **ONLY** when absolutely necessary; e.g., a special agent is assaulted or if a felony violation occurs in their presence.

20.5.b.(3). Determine and comply with procedures of the local U.S. Attorney, U.S. Marshal, and U.S. District Court regarding arrests. When applicable, consult with the prosecutor and duty magistrate to determine the timing of the arrest.

20.5.b.(4). Plan carefully all arrest situations by considering the following:

20.5.b.(4).(a). safety of special agents;

20.5.b.(4).(b). safety of the public;

20.5.b.(4).(c). safety of the prisoner;

20.5.b.(4).(d). secure transportation of the prisoner to the magistrate;

20.5.b.(4).(e). processing the prisoner;

20.5.b.(4).(f). temporary detention of the prisoner at a U.S. Bureau of Prisons-approved facility before arraignment;

20.5.b.(4).(f).1. whenever possible, advise the U.S. Marshals Service (USMS) office as soon as you know where and when you will be making an arrest. The USMS office will advise you where you may lodge a prisoner if you are unable to get to a magistrate before close of business. In most situations, the arresting special agent, not the USMS, assumes responsibility for a Federal prisoner until the time of arraignment before a U.S. Magistrate;

20.5.b.(4).(f).2. contact the local USMS office to determine the location of and obtain directions to the nearest medical facility that has an authorized ward to hold Federal prisoners in case the arrestee requires medical treatment;

20.5.b.(4).(g). sufficient personnel and equipment to effect arrest safely.

(b)(7)(E)

20.5.b.(4).(h). coordination with local law enforcement agencies;

20.5.b.(4).(i). special considerations; e.g., the need for foreign or sign language interpretation, having a special agent of the same sex as the person arrested conduct the search of the person;

20.5.b.(4).(j). safe and secure handling and storage of all confiscated property.

20.5.b.(5). Should the arrestee require medical clearance/treatment for any preexisting medical condition, or from injuries sustained incident to the arrest (e.g., exposure to pepper spray, contusions), the special agent shall take the following actions, as necessary.

20.5.b.(5).(a). Transport the arrestee to the nearest medical facility that has an authorized ward to hold Federal prisoners, in case the arrestee requires admission for further treatment. Special agents should contact the local USMS office for verification of approved medical facilities.

20.5.b.(5).(b). Physically accompany the arrestee in the ambulance to the appropriate medical facility when, based on medical necessity, the arrestee requires transportation by ambulance. If, however, based on the urgency of the situation, and/or the medical necessities of the transporting entity, it is impractical for the special agent to accompany the arrestee, the special agent shall immediately proceed to the medical facility.

20.5.b.(5).(c). Notify his/her respective supervisor.

20.5.b.(5).(d). Obtain copies of all billings for forwarding to the Special Agent in Charge, Investigative Operations Directorate, who upon receipt will forward the billings through the Office of General Counsel to the Office of the Chief of Staff for payment processing.

20.5.b.(5).(e). Contact the local U.S. Attorney's Office and USMS office for procedures regarding detention and arraignment procedures for that judicial district of in-custody medical admissions at the respective medical facility.

20.5.b.(6). Ensure the arrestee's data is entered into the National Crime Information Center (NCIC) upon issuance of the arrest warrant and prior to effecting the arrest.

20.5.b.(7). Identify yourself by displaying your badge and credentials at the earliest possible opportunity, consistent with safety during the arrest process.

(b)(7)(E)

20.5.b.(9). Advise the prisoner of his/her constitutional rights, if you intend to question the prisoner. If the case involves Service members, advise them of their rights under the Uniform Code of Military Justice. See SAM Chapter 5, "Rights Warnings," and DCIS Forms 6, 7, 71, and 70.

20.5.b.(10). Inventory the personal property of the prisoner at the first appropriate opportunity. If the prisoner was arrested in or near a motor vehicle, secure it at the scene or arrange for its safe storage with the local law enforcement agency. Vehicles should be stored at a secure location or a facility used by other law enforcement agencies. If adequate facilities are unavailable, contact the U.S. Marshal to arrange for storage. Make every effort to avoid assuming custody of vehicles, unless warranted by circumstances of the arrest.

20.5.b.(10).(a). Inventory all vehicles and their contents, and all other property taken into custody. Conduct an inventory to:

20.5.b.(10).(a).1. protect the owner's property while in Government custody;

20.5.b.(10).(a).2. protect the Government against claims of lost, stolen, or vandalized property; and

20.5.b.(10).(a).3. protect DCIS personnel from potentially dangerous items.

20.5.b.(10).(b). The inventory shall be conducted at the time of the arrest, or as soon thereafter as circumstances allow, and shall consist of opening all compartments, including locked or closed containers, and cataloging all items found. An inventory list shall be prepared as an attachment to the Arrest Report Form 1 showing the results of the inventory. Use DCIS Form 20-2, DCIS Vehicle Inspection Form (Attachment A), as the inventory list.

20.5.b.(10).(c). Vehicle inventory lists should include, but not be limited to, the following:

20.5.b.(10).(c).1. description of the vehicle (year, make, model, color, vehicle identification number, license number);

20.5.b.(10).(c).2. description of all valuables secured from a vehicle for safekeeping;

20.5.b.(10).(c).3. list of all accessories, tools, and unattached parts left in the vehicle;

20.5.b.(10).(c).4. notation describing the condition of the body and upholstery (specifically naming the damage or deteriorated areas and briefly stating the extent of the damage); and

20.5.b.(10).(c).5. list of all missing items such as keys, motor, radio, battery, spare tire, etc.

20.5.b.(10).(d). Place the original inventory list (DCIS Form 20-2) in the investigative case file with a copy attached to or left with the property, a copy provided to the representative of the storage facility, and a copy provided to the person from whom the property was seized.

20.5.b.(10).(e). Minimize damage to a container or its contents while gaining access, in the event a container or vehicle compartment is locked or sealed.

20.5.b.(10).(f). Seize all property discovered in the course of a property inventory that constitutes contraband or evidence of a crime. Follow the evidence handling, inventory, and receipt procedures in SAM Chapter 18, “Evidence Custody System,” for any evidence or contraband seized.

20.5.b.(11). Before transporting a prisoner to the magistrate, you are allowed a reasonable time (as determined by the magistrate) to obtain fingerprints, photographs, a DNA sample, and a personal history from an arrested person. However, prolonged interrogation during processing may be considered an unnecessary delay in transporting the prisoner to the magistrate. A delay of more than 6 hours will probably be considered excessive unless there are extenuating circumstances (18 U.S.C. §3501(c)).

20.5.b.(11).(a). Take fingerprints on two FBI Forms FD-249, Standard Criminal Fingerprint Card (Attachment B), and one FBI Form R-84, Final Disposition Report (Attachment C), following the instructions on the forms. File one fingerprint card in the case file and forward one fingerprint card to the FBI Identification Division. Save the Form R-84 to report the final disposition of the criminal charges to the FBI at the appropriate time.

20.5.b.(11).(b). If fingerprints are taken by the USMS or another investigative agency, make sure the “Send copy to” box has the correct DCIS office address and the NCIC alphanumeric routing identifier (commonly referred to as the “ORI number”) so that DCIS will receive a copy of any criminal history.

20.5.b.(11).(c). Take two full-face (head and shoulders) and two profile color photographs. Record the case number, the prisoner’s name, and the date on the reverse of the photographs and file them in the case file with the fingerprint card.

20.5.b.(11).(d). In a judicial district in which there is an adverse decision by a district judge that has not yet been corrected on appeal, DCIS must suspend DNA sample collection from arrestees in that judicial district in the absence of a supporting court order for collection in a specific individual case. This will protect DCIS agents in that district from accusations and potential lawsuits charging that they have violated the alleged right of arrestees to be free of DNA sample collection, as declared in the adverse decision (see Attachment D). In all other instances, in accordance with Department of Defense Instruction 5505.14, “DNA Collection Requirements for Criminal Investigations,” May 27, 2010, and as outlined in the “Buccal Kit Training Presentation” (see S:\DCIS\Use of Force Program\DNA Collection\USACIL DNA Collection Training PP), DNA samples shall be collected and forwarded to the U.S. Army Criminal Investigation Laboratory (USACIL) when:

20.5.b.(11).(d).1. fingerprints are taken in connection with an investigation in which the special agent concludes there is probable cause to believe that the subject is a Service member and has committed the offense under investigation. The special agent must consult with a prosecuting attorney or judge advocate prior to making a probable-cause determination. Samples may be collected, but not forwarded, prior to consultation. DNA shall not be taken for the wrongful use of a controlled substance, nor shall it be taken for the wrongful possession of a controlled substance when the controlled substance possessed:

20.5.b.(11).(d).1.a. is not intended for distribution;

20.5.b.(11).(d).1.b. is not possessed in connection with wrongful importation or exportation;

20.5.b.(11).(d).2. court-martial charges are preferred in accordance with Rule for Courts Martial (RCM) if a DNA sample has not already been submitted;

20.5.b.(11).(d).3. a member is ordered into pre-trial confinement by a competent military authority after the completion of the commander's 72-hour memorandum if a DNA sample has not already been submitted;

20.5.b.(11).(d).4. a member is confined to a military correctional facility or temporarily housed in civilian facilities as a result of any general or special court-martial conviction if a DNA sample has not already been submitted.

20.5.b.(11).(e). DCIS will take DNA samples from civilians they detain or hold and who remain within their control at the point it is determined there is probable cause to believe the civilian has violated any provision of Federal law that requires an in-court appearance. DNA samples may also be taken by civilian law enforcement organizations; however, an individual DNA sample does not need to be taken more than once.

20.5.b.(11).(f). DNA samples taken by DCIS shall be forwarded to USACIL. The special agent shall document in the appropriate case file when civilian law enforcement organizations handle any aspect of the DNA processing and whether the civilian law enforcement agency forwarded the DNA sample to the FBI Laboratory. This reference does not require DCIS to take samples from a civilian not in their control at the point when a probable cause determination is made.

20.5.b.(11).(g). Service members and civilians from whom samples were taken and forwarded to USACIL or the FBI, but who are not convicted of any offense, may request in writing that their DNA records be expunged. Instructions for this procedure are found in DoD Instruction 5505.14.

20.5.b.(11).(h). Prepare a DCIS Form 1 documenting the arrest. Attach a copy of the arrest warrant and complaint. The "Remarks" section of the Arrest Report Form 1 must provide information concerning identities of all special agents present, what was observed, what duties were performed, and any statements made by the arrested person. Any use of force must be described in detail in the Arrest Report Form 1 (example at Attachment E). If the arrested person is covered as a significant incident in accordance with DoD Instruction 5240.4, "Counterintelligence (CI) Investigations," February 2, 2009, the arrest should be submitted to Headquarters as a Significant Incident Report Form 1.

20.5.b.(11).(i). Enter the arrest and identifying data in the DCIS Investigative Data System, as specified in SAM Chapter 50. “Investigative Data System.”

20.5.b.(11).(j). Personal property should be transferred along with the prisoner (other than items of evidence or contraband, which must be entered into the Evidence Custody System). If this is not possible, ensure that such property is placed in a locked or other secured facility. With regard to the disposition of vehicles, see paragraph 20.5.b.(10).

20.5.b.(11).(k). See SAM Chapter 22, “Juveniles and Criminal Investigations,” regarding the arrest of and handling of juveniles.

20.6. Non-Federal Crimes. There is no Federal authority for special agents to intervene in non-Federal crimes. Unless special status is conferred by state legislation, special agents intervening in state crimes do so as ordinary citizens.

20.6.a. Pursuant to 28 U.S.C. 2671, commonly known as the Law Enforcement Officers’ Good Samaritan Act, *for the purpose of tort liability*, a DCIS Special Agent shall be construed to be acting within the scope of his or her office, or employment, if the special agent takes reasonable action, including the use of force (see SAM Chapter 38 regarding the use of force), to:

20.6.a.(1). protect an individual from a crime of violence, if that crime has been committed in his or her presence;

20.6.a.(2). provide immediate assistance to an individual who has suffered or is threatened with bodily harm; or

20.6.a.(3). prevent the escape of any individual that the special agent reasonably believes to have committed a crime of violence, if that crime has been committed in his or her presence.

20.6.b. Pursuant to 18 U.S.C. 16, the term “crime of violence” means:

20.6.b.(1). an offense that has as an element the use, attempted use, or threatened use of physical force against the person or property of another; or

20.6.b.(2). any other offense that is a felony and that, by its nature, involves a substantial risk that physical force against the person or property of another may be used in the course of committing the offense.

20.6.c. In the event that a special agent’s intervention in a state or local crime situation involves the use of force and results in serious physical injury or death, emergency, interim legal representation may be available from private counsel at Government expense. See SAM Chapter 38, Attachment A, “Procedures for Obtaining Emergency Legal Representation for DCIS Personnel Involved in Critical Incidents.”

ATTACHMENTS

<u>Attachment</u>	<u>Title</u>
A	DCIS Form 20-2, Vehicle Inspection Form
B	FBI Form FD-249, Standard Criminal Fingerprint Card
C	FBI Form R-84, Final Disposition Report
D	Attorney General Guidelines, "DNA Sample Collection from Federal Arrestees and Defendants"
E	Sample Arrest Report Form 1



MEMORANDUM

TO: ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION
ASSISTANT ATTORNEY GENERAL, NATIONAL SECURITY DIVISION
ALL UNITED STATES ATTORNEYS
DEPUTY DIRECTOR OF THE BUREAU OF ALCOHOL, TOBACCO,
FIREARMS AND EXPLOSIVES
ACTING ADMINISTRATOR OF THE DRUG ENFORCEMENT
ADMINISTRATION
DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION
DIRECTOR OF THE UNITED STATES MARSHALS SERVICE

FROM: Eric H. Holder, Jr.
Attorney General

SUBJECT: DNA Sample Collection from Federal Arrestees and Defendants

DNA identification is a landmark advance in law enforcement identification technology, comparable in significance to the historical development of fingerprint identification and photographic identification methods. DNA provides a powerful new tool in the enforcement of federal and state criminal laws and the administration of justice, helping both to bring the guilty to justice and to protect the innocent from mistaken suspicion, accusation, and conviction. As with other forms of identification information that are taken from persons who enter the justice system, including fingerprints and photographs, the value of DNA identification information is maximized by obtaining it at the earliest feasible point in the criminal justice process. Accordingly, the regular collection of DNA samples from federal arrestees and defendants must be a priority.

The purpose of this memorandum is to review with federal prosecution offices and Department of Justice investigative agencies the requirement to collect DNA samples from federal arrestees and defendants and to provide guidance concerning issues that have arisen in the implementation of this requirement. The matters discussed include the general requirement to collect DNA samples, the status of implementation of the requirement and the treatment of cases in which an arresting agency is unable to collect a sample, and situations in which implementation is impeded by adverse judicial decisions.

I. THE DNA SAMPLE COLLECTION REQUIREMENT

Federal law has required the collection of DNA samples from most persons *convicted* of federal crimes since 2004, and more recent developments have extended DNA collection to include arrestees and defendants in the federal jurisdiction.¹ Specifically, the DNA Fingerprint Act, enacted in 2006, authorized the Attorney General to implement this reform. See 42 U.S.C. § 14135a(a)(1)(A). The Attorney General exercised this authority in 28 C.F.R. § 28.12, as amended by the rulemaking at 73 Fed. Reg. 74932.²

The rule, which went into effect on January 9, 2009, in part directs federal agencies to “collect DNA samples from individuals who are arrested, facing charges, or convicted . . . under the authority of the United States.” 28 C.F.R. § 28.12(b). In relation to persons arrested for or charged with federal crimes, the effect is to add DNA to the types of identification information that are routinely taken in booking, generally on a par with fingerprinting.

The DNA Fingerprint Act also enacted complementary changes in 18 U.S.C. § 3142(b), (c)(1)(A), making cooperation in DNA sample collection a mandatory condition of pretrial release. Moreover, failure to cooperate in such collection is independently a federal crime, as provided in 42 U.S.C. § 14135a(a)(5).

The authorized method of DNA sample collection from non-convicts in the federal jurisdiction is by buccal (cheek) swab. The FBI provides buccal swab kits without charge to the agencies responsible for sample collection for this purpose, and the completed kits are returned to the FBI Laboratory for analysis and entry of the resulting DNA profiles into the Combined DNA Index System (CODIS).³ Instructions for ordering and using the buccal swab kits are available on the FBI’s website. See www.fbi.gov/about-us/lab/dna-nuclear/nuclear-dna, under links “Buccal Kit Collection Instructions” and “Buccal Collection Kit Re-Order Form.”

II. IMPLEMENTATION

The principal investigative agencies of the Department of Justice—FBI, DEA, ATF, and USMS—have implemented the DNA Fingerprint Act and 28 C.F.R. § 28.12 as amended and are collecting DNA samples from their arrestees. Investigative agencies in other Departments are at varying stages in their implementation efforts.

As noted, cooperation in DNA sample collection is a mandatory condition of pretrial release in federal cases. This condition is moot if the arresting agency has already taken a DNA sample in booking, prior to the defendant’s initial appearance in court.

¹ Almost all of the states similarly collect DNA samples at least from all convicted felons, and over 20 states also authorize DNA sample collection from various non-convict (arrestee or defendant) classes.

² The preamble to the rule provides extensive information about the background, rationale, and operation of the current DNA sample collection policy, discussion of related legal and policy matters, and responses to objections. See 73 Fed. Reg. 74932-42.

³ The Department of Defense is an exception, not relying on the FBI for these purposes because it has its own capacity to prepare DNA sample collection kits and to derive DNA profiles for persons in the military justice system.

In some cases, however, defendants will appear in court without having previously provided DNA samples. This may occur for various reasons. One reason is that in some cases arrestees may refuse to cooperate in DNA sample collection in booking. In such a case, the arresting agency may judge that the most appropriate response is to forgo DNA collection at the booking stage, and instead to bring the arrestee to court. Another possible reason is that the arresting agency may not yet have implemented arrestee DNA sample collection as a general matter. For example, the Department of Homeland Security has advised that additional time will be needed to implement arrestee DNA sample collection by its agencies. Whatever the reason, if a defendant appears in court without prior collection of a DNA sample, the court can then order the defendant to cooperate in such collection as a mandatory pretrial release condition under 18 U.S.C. § 3142(b), (c)(1)(A), and as necessary to abate the defendant's commission of the crime of non-cooperation in DNA sample collection under 42 U.S.C. § 14135a(a)(5).

For cases in which the arresting agency has not collected a DNA sample and is unable to do so following the defendant's production in court, the U.S. Attorney's Office should attempt to coordinate with other agencies to seek their assistance in taking the buccal swab. The district courts may be amenable to general arrangements under which the U.S. Probation or Pretrial Services Office will function as the default DNA sample collection agency in cases where an executive agency is unable to carry out this function. The Probation Offices have collected DNA (in the form of blood samples) from convicted offenders under their supervision for many years, *see* 42 U.S.C. § 14135a(a)(2). The Probation and Pretrial Services Offices are similarly subject to the current requirement that federal agencies that supervise persons facing charges collect DNA samples, *see* 73 Fed. Reg. 74940, with the proviso that the authorized form of DNA sample collection from non-convicts is buccal swab rather than blood sample, as noted above. The Probation and Pretrial Services Offices may order buccal swab kits from the FBI and use them in the same manner as executive agencies.

III. ADVERSE DECISIONS

The U.S. Attorney's Office should inform its Criminal Division, Appellate Section contact regarding challenges to DNA sample collection from arrestees or defendants. The issue has been litigated in a number of cases with mixed results. In *United States v. Pool*, 621 F.3d 1213 (9th Cir. 2010), the Ninth Circuit Court of Appeals rejected a constitutional challenge to DNA sample collection from federal arrestees and defendants, affirming a district court decision reported at 645 F.Supp.2d 903 (E.D. Cal. 2009) and 2009 WL 2152029 (E.D. Cal. July 15, 2009). In *Haskell v. Brown*, 677 F.Supp.2d 1187 (N.D. Cal. 2009), the district court rejected a constitutional challenge to California's provision for DNA sample collection from arrestees, a provision that presents essentially the same issues as the federal statute and rule. On the other side, in *United States v. Mitchell*, 681 F.Supp.2d 597 (W.D. Pa. 2009), the district court held that the federal statute and rule are unconstitutional. The case is pending on the Government's appeal before the Third Circuit. A second adverse decision is *United States v. Frank*, No. 2:09-cr-2075 (E.D.Wash. Mar. 10, 2010).

In the event of an adverse decision by a district judge regarding the validity of 42 U.S.C. § 14135a(a)(1)(A) or its implementing rule, the U.S. Attorney's Office may continue to press the

issue in litigation before other judges in the district. Alternatively, the U.S. Attorney's Office may conclude that further efforts to enforce the DNA sample collection requirement at the district court level would likely be unproductive and should be suspended during the pendency of an appeal of the adverse decision to the Court of Appeals. This is an issue of effective litigation strategy that the USAO should decide in consultation with the Criminal Division, Appellate Section contact.

In a district in which there is an adverse decision by a district judge that has not yet been corrected on appeal, investigative agencies must suspend DNA sample collection from arrestees in that district in the absence of a supporting court order for collection in a specific, individual case. This will protect investigative agents in that district from accusations and potential lawsuits charging that they have violated the alleged right of arrestees to be free of DNA sample collection, as declared in the adverse decision.

An adverse district court decision in a particular district regarding DNA sample collection does not affect the collection of DNA samples in other districts. Investigative agencies should continue to collect DNA samples from their arrestees elsewhere and federal prosecutors should continue to insist that defendants be required to cooperate in DNA sample collection in litigation in other districts.

Further questions about the DNA sample collection policy and its implementation may be directed to Anne Pings, EOUSA, Legislative Counsel, telephone: 202-252-1435, email: Anne.Pings@usdoj.gov.



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

November 26, 2013

INSPECTOR GENERAL INSTRUCTION 1432.1

INCENTIVE AND HONORARY AWARDS PROGRAM

FOREWORD

This Instruction provides the basic instructions required for the management of the Department of Defense Office of Inspector General Incentive and Honorary Awards Program.

The Incentive and Honorary Awards Program prescribes policies, procedures, guidelines, and program responsibilities. This Instruction describes Office of Inspector General incentive and honorary awards, Department of Defense honorary awards, and other awards available or not available to Office of Inspector General career and non-career Federal employees, non-Office of Inspector General career and non-career Federal employees, military members, private citizens, contractors and foreign nationals.

This Instruction must be reissued, cancelled, or certified current within 5 years of its publication date, in accordance with Department of Defense Instruction 5025.01, *Department of Defense Directives Program*. If not, it will expire 10 years from its publication date and will be removed from the Office of Inspector General website.

The office of primary responsibility for this Instruction is the Human Capital Advisory Services Directorate. This Instruction is effective immediately.

FOR THE INSPECTOR GENERAL:

A handwritten signature in black ink, appearing to read "SD Wilson", is positioned above the printed name.

Stephen D. Wilson
Assistant Inspector General
for Administration and Management

CHAPTER 22

JUVENILES AND CRIMINAL INVESTIGATIONS

<u>Contents</u>	<u>Section</u>
General	22.1.
Policy	22.2.
Definitions	22.3.
Determining Whether the Individual Is a Juvenile	22.4.
Arrests	22.5.
Interviews and Interrogations	22.6.
Juvenile Witnesses	22.7.
Parental Notification	22.8.
Photographing and Fingerprinting	22.9.
Psychophysiological Detection of Deception (PDD)	
Examination	22.10.
Publicity	22.11.
Release of Information	22.12.
Search and Seizure	22.13.
Confidential Informants	22.14.
Titling of Juveniles in DCIS Forms 1 and Entering Information into CRIMS	22.15.

22.1. General. This chapter prescribes policies and procedures on dealing with juveniles in connection with investigations conducted by special agents of the Defense Criminal Investigative Service (DCIS), Office of the Inspector General, Department of Defense. Most DCIS investigative activities do not involve juveniles and those investigative activities involving juveniles do not typically require taking the juveniles into custody. However, all agents must be aware of the unique status of juveniles and must follow the provisions as set forth in the Juvenile Justice and Delinquency Prevention Act of 1974, Title 18, United States Code (U.S.C.), Sections 5031-5042 (Juvenile Delinquency Act). The statute delineates who is considered a juvenile under Federal law, when a juvenile may be treated as a juvenile delinquent in Federal court, when a juvenile may be prosecuted as an adult in Federal court, and the procedures to be followed in each case.

22.2. Policy

22.2.a. From the outset of an investigation, there is a need to exercise certain precautions when proceeding against a juvenile. The interview and/or interrogation of juvenile suspects is limited by applicable provisions of the Juvenile Delinquency Act. Whenever the custody, or implied custody, of a juvenile is effected, the requirements and restrictions of the Juvenile Delinquency Act apply.

22.2.b. The following procedures apply to all DCIS agents wherever located.

22.3. Definitions. The following definitions apply as used in this chapter.

22.3.a. **Custody.** The placing of an individual under arrest or otherwise restricting the individual's freedom of action in any significant way.

22.3.b. **Interrogation.** Any formal or informal questioning in which an incriminating response is either sought or is a reasonable consequence of such questioning; typically the questioning of a suspect.

22.3.c. **Interview.** The questioning of an individual who either has or is believed to have factual information, not self-incriminating, that is of interest to the investigator. An interview is the questioning of a witness, as compared to an interrogation, which is used to question a subject/suspect. See Chapter 4, "Interviews and Interrogations," DCIS Special Agents Manual (SAM), for further policy and guidance.

22.3.d. **Juvenile.** A person under 18 years of age.

22.3.e. **Juvenile Delinquency.** A violation of a law of the United States committed by a person prior to his or her 18th birthday that would have been a crime if committed by an adult. A person over 18 years of age but less than 21 years of age is also accorded juvenile treatment if the act of juvenile delinquency occurred prior to his or her 18th birthday.

22.3.f. **Minor.** A person under 18 years of age.

22.3.g. **Subject/Suspect.** A person whose involvement in the commission of some violation of existing law is considered, on reasonable grounds, to be a practical possibility.

22.4. Determining Whether the Individual Is a Juvenile. A recurrent issue in juvenile proceedings is whether the subject of an investigation was under the age of 18 at the time of the offense and whether he or she is now under 21 for the purpose of juvenile delinquency proceedings. If you have a question concerning the subject's age and the subject has no undisputed proof of birth date to offer, the Federal courts have held that the burden of proof is on the person claiming the benefit of the Federal juvenile statutory provisions, especially since that person is in the best position to offer evidence of his or her age. On the other hand, if the exact date of the offense is the critical issue, that burden will be placed on the prosecutor.

22.5. Arrests

22.5.a. If an agent anticipates that a juvenile will be arrested or that the agent will seek pretrial detention, the agent should provide as much notice as possible to the United States Marshals Service so they can begin to determine the availability of local contract juvenile bed space. Since the U.S. Marshals Service currently contracts for juvenile bed space with state, local, and private organizations on an "as needed" basis, it is recommended that they have as much lead time as possible to locate an appropriate custodial facility.

22.5.b. When an arrest is made of a juvenile, the arresting agent should immediately advise the juvenile of his or her rights in language intelligible and comprehensible to the juvenile.

22.5.c. The arresting agent must immediately notify the Assistant United States Attorney (AUSA) and the juvenile's parent(s), guardian, or custodian of the arrest. The parent(s), guardian, or custodian must also be notified of the juvenile's rights and the nature of the alleged offense.

22.5.d. The juvenile must be taken before a magistrate as soon as possible and within a reasonable period of time. The courts have varied interpretations on what constitutes "a reasonable period of time," so it is essential that the agent consult with the AUSA to determine the law of your district.

22.5.e. A separate DCIS Form 1 should be prepared to clearly document that:

22.5.e.(1). the juvenile was advised of his or her rights;

22.5.e.(2). the AUSA was notified;

22.5.e.(3). the parent(s), guardian, or custodian was notified; and

22.5.e.(4). the juvenile was promptly taken before a magistrate.

22.5.f. The arrest and identifying data is to be entered into the DCIS Case Reporting and Information Management System (CRIMS), as specified in SAM Chapter 50.

22.6. Interviews and Interrogations

22.6.a. **Questioning a Juvenile.** The questioning of juvenile suspects raises legal issues that could have a bearing on the admissibility of any confession made by a juvenile in custody. A juvenile has both a right to counsel and a privilege against self-incrimination in juvenile delinquency proceedings. A juvenile may waive his or her Fifth Amendment rights and consent to interrogation. The question of whether a waiver is voluntary and knowing is one to be resolved on the totality of the circumstances surrounding the interrogation. The courts will determine whether the statements were coerced or suggested, and also whether they were the products of "ignorance of rights or of adolescent fantasy, fright or despair."

22.6.b. **Factors to Consider.** When interviewing or interrogating juveniles, important factors to take into consideration are the juvenile's age, experience, education, background, intelligence, and whether he or she has the capacity to understand the warnings given to him or her, the nature of his or her Fifth Amendment rights, and the consequences of waiving them.

22.6.c. **Warning.** Since confessions by juveniles are given even closer scrutiny than those by adults, the Miranda warning is an essential threshold requirement for voluntariness of

statements and is required if the subject is in custody. The presence and co-signature of a parent or guardian is not required for a voluntary waiver, although it is a factor to be considered and will help dispel any notion that the juvenile was coerced.

22.6.d. Interviews

22.6.d.(1). As a general rule, juveniles will be interviewed in a noncustodial setting.

22.6.d.(2). The parent(s), guardian, or their designated representative normally should be present during the interview of their minor children and should, if possible, provide their consent in writing for the interview to be conducted.

22.6.d.(3). The juvenile and parent(s) will be advised that they may terminate the interview at any time.

22.6.d.(4). It must be clearly demonstrated that the juvenile's cooperation is voluntary.

22.6.e. Interrogations

22.6.e.(1). The parent(s) or guardian of the juvenile will be advised of the interrogation rights of the juvenile.

22.6.e.(2). The juvenile will be advised of his rights against self-incrimination with the consent of the parent or guardian.

22.6.e.(3). The juvenile and parent(s) will be advised that they may terminate the interview at any time.

22.7. Juvenile Witnesses. Before transporting or having a juvenile witness transported to a DCIS office or other law enforcement activity for an interview, a parent or responsible guardian should be notified. In addition, the agent should make every effort to ensure that a juvenile has transportation to and from the DCIS office or other law enforcement activity prior to setting up an interview if DCIS will not be providing the transportation. Prior parental/guardian notification is not necessary during interviews at crime scenes, during area canvasses, etc. When transporting juveniles, agents should be accompanied by another law enforcement officer, preferably of the same sex as the juvenile, if available.

22.8. Parental Notification

22.8.a. From the moment a juvenile is detained, he or she is entitled to juvenile custody and notification of parent(s). By statute, the agent arresting a juvenile is required to advise a juvenile of his rights, and must immediately notify an Assistant U.S. Attorney and the juvenile's parent(s), guardian, or custodian of such custody. The arresting agent is also required to notify

the parents, guardian, or custodian of the rights of the juvenile and the nature of the alleged offense. The juvenile must be taken before a magistrate as soon as possible and within a reasonable period of time.

22.8.b. If the juvenile is a non-naturalized citizen, a reasonable effort must be made to reach his or her parent(s). If this is not feasible, prompt notice should be made to his or her country's consulate.

22.9. Photographing and Fingerprinting

22.9.a. The Juvenile Delinquency Act states that no juvenile who has been arrested shall be photographed unless it is determined that the juvenile will be tried as an adult, or the U.S. District judge consents to the photograph being taken. This prohibition is applicable to DCIS agents, the U.S. Marshals Office, and any local facility in which a juvenile is incarcerated on Federal charges.

22.9.b. When the parent of the juvenile is the suspect/subject of an offense against the juvenile, the juvenile may be photographed in order to document instances of abuse and/or negligence, provided the juvenile does not object.

(b)(7)(E)

22.9.d. The Juvenile Delinquency Act provides for fingerprinting of a juvenile only after a finding of guilt for certain types of drug and violent offenses. Because it will not be known at the time of an arrest whether the juvenile will be prosecuted as an adult or handled as a juvenile offender, agents are not to fingerprint without the consent of the U.S. District judge.

22.9.e. Fingerprinting a juvenile for general purposes will not be done unless there is written consent from a U.S. District judge responsible for juvenile cases, regardless of consent by the juvenile or the parents and/or guardian.

22.10. Psychophysiological Detection of Deception (PDD) Examination. The PDD, or polygraph, examiner cannot conduct a competent examination, and by regulation, is prohibited from conducting a PDD examination when, in the examiner's opinion, the person fits one of the following descriptions:

22.10.a. the person is below the age of reason; or

22.10.b. young children who have not matured to the extent of fully understanding social responsibilities are not suitable subjects for the PDD technique.

22.11. Publicity

22.11.a. Press releases and other publicity identifying a juvenile directly or indirectly are not permitted under 18 U.S.C. 5038.

22.11.b. If a person is belatedly determined to be a juvenile (after publicity or indictment) and if a hearing on a motion to transfer the juvenile to adult status is not imminent, efforts should be made to minimize further publicity.

(b)(7)(E)

22.13. Search and Seizure. As a general rule, parents may consent to the search of a family dwelling directed against juveniles residing therein and being supported by the parents. On the other hand, since Fourth Amendment protection belongs to the parents, juveniles may not relinquish the parents' rights by consenting to a search of the family home directed against them.

22.14. Confidential Informants

22.14.a. The use of confidential informants in law enforcement is both a time honored and constitutionally acceptable method of collecting information and identifying substantive criminal activities.

(b)(7)(E)

22.15. Titling of Juveniles in DCIS Forms 1 and Entering Information into CRIMS

22.15.a. Titling juveniles in case initiations, Forms 1, case summaries, and Reports of Investigation is permissible but the documents must be marked in order to provide extra protection from release as required by 18 U.S.C. 5038.

22.15.b. When titling juveniles, agents should follow the guidance provided in SAM Chapter 28, “Investigative Reports,” regarding titling persons.

22.15.c. Special agents should enter the identifying data concerning juveniles in the DCIS CRIMS, following the guidance specified in SAM Chapter 50. CRIMS will automatically flag a subject record as a juvenile if the date of birth entered is less than 18 years old from the “Created On” date for the subject record. To comply with the provisions of 18 U.S.C. 5038, when an adjudicative action on a juvenile subject is under a court seal, no action will be reported in CRIMS.

22.15.d. Any documents prepared that contain the name of a juvenile should be marked with the following:

NOTICE: This document contains information on a juvenile and should be protected from unauthorized release.

22.15.e. If it is determined later during the course of the investigation that the subject is a juvenile, the case documents do not need to be rewritten but need to be safeguarded against release to unauthorized individuals. All future documents containing information about a juvenile would need to be marked with the above notice.

CHAPTER 23

VICTIM AND WITNESS ASSISTANCE

<u>Contents</u>	<u>Section</u>
General	23.1.
Definitions	23.2.
Responsibilities	23.3.
Victim and Witness Assistance	23.4.
Procedures	23.5.
Victim Compensation and Expenditures	23.6.
Victim/Witness Protection Procedures	23.7.
Reporting Requirements	23.8.
Other Types of Victims	23.9.

23.1. General. This chapter provides uniform policies and procedures for implementing the Victim and Witness Assistance Program (VWAP) within DCIS. This chapter incorporates DoD Directive 1030.01, “Victim and Witness Assistance,” issued April 13, 2004, and DoD Instruction 1030.2, “Victim and Witness Assistance Procedures,” issued June 4, 2004. The DoD Directive and Instruction incorporate requirements from the Victim’s Rights and Restitution Act (VRRRA) § 503, Title 42, United States Code (U.S.C.) § 10607 (2006) and the Victim and Witness Protection Act § 4(a), 18 U.S.C. §§ 1512-1514. Additionally, because DCIS works closely with the Department of Justice (DOJ), agents should be familiar with the more comprehensive standards set forth in the DOJ “Attorney General Guidelines for Victim and Witness Assistance” (AG Guidelines) of October 2011 (Attachment A). The core statutes included in the AG Guidelines are the VRRRA and the Crime Victims’ Rights Act (CVRA), 18 U.S.C. § 3771. The purpose of this chapter is to provide guidance to DCIS special agents and other employees whose duties may impact victims/witnesses in DCIS investigations. DCIS’s designated National Victim Witness Coordinator and, where appropriate, the Victim Witness Coordinator at the local U.S. Attorney’s Offices, shall be consulted on an as needed basis.

23.2. Definitions

23.2.a. **Victim.** For purposes of providing services to crime victims, under 42 U.S.C. §10607 (e)(2), a victim is defined as “a person that has suffered direct physical, emotional, or pecuniary harm as a result of the commission of a crime.” If a victim is an institutional entity, services may be provided to an authorized representative of that entity. Only those persons suffering direct physical, emotional, or pecuniary harm are considered victims for purposes of the DCIS Victim Witness Assistance Program (VWAP). Thus, persons whose injuries are indirectly caused by the crime are not entitled to services. Bystanders are generally not considered victims although there may be circumstances when a bystander does suffer direct injury, and DCIS employees shall treat the bystander as a victim. This does not prohibit DCIS employees from assisting persons affected indirectly, to the extent deemed appropriate.

23.2.b. **DoD Victim/Witness Brochure (DD Form 2701).** This brochure, otherwise referred to as DD Form 2701, “Initial Information for Victims and Witnesses of Crime,” is to be used by all DCIS special agents and other DoD law enforcement personnel, as appropriate, to inform victims and witnesses of a crime of certain rights and points of contact within the criminal justice and victim/witness support systems. The blanks on the back of the brochure should be filled in by the case agent or other responding agent, as appropriate, and given to all victims of crimes investigated by DCIS. Information regarding coordination of compensation to the victim for medical or other expenses is also included in the brochure, which suggests coordination with the applicable state office for Crime Victim Compensation. Otherwise, coordination of payment for medical or other services will occur through the field office Special Agent in Charge (SAC) to the SAC, Internal Operations. If jurisdiction resides with another agency and that agency has provided victims with similar information, then DCIS does not have to duplicate the effort. The case agent must be sensitive to the needs of the victims and provide those victims with a copy of the brochure whenever, in the agent’s judgment, it may be in the best interest of the victim or witness to do so. The DD 2701 should be reproduced locally. Attachment B contains a blank DD 2701 and Attachment C contains an example of a completed DD 2701.

23.2.c. **National/Headquarters (HQ) VWAP Coordinator.** The National (i.e., DCIS HQ) VWAP Coordinator will be responsible for the annual collecting of DCIS VWAP statistical information from field offices and providing this information to the SAC, Internal Operations, by means of a DD Form 2706, Annual Report on Victim and Witness Assistance (Attachment D). The DCIS HQ VWAP Coordinator is designated by the SAC, Internal Operations, and is under the Internal Operations directorate. The SAC, Internal Operations, will subsequently submit this information to the DoD Legal Policy Office, 4000 Defense Pentagon, Washington, DC 20301-4000, prior to **March 15** as required by DoD Instruction 1030.2. The HQ VWAP Coordinator will also identify and participate in annual training, as available and budget permitting, relevant to this duty and will assist Internal Operations in establishing and coordinating training for field components, as needed.

23.3. Responsibilities

23.3.a. **Agent.** The following are the special agent’s responsibilities pertaining to victims.

23.3.a.(1). Identify all victims of crimes under investigation.

23.3.a.(2). Provide the victim/witness with a DD Form 2701 and all services or information required by law (see sections 23.1. and 23.2.) for all victims/witnesses.

23.3.a.(3). Keep field management apprised of any issues that may require additional resources, management, or National Victim/Witness Coordinator guidance or involvement.

23.3.a.(4). Inform victims/witnesses of how to contact the appropriate U.S. Attorney’s Victim/Witness Coordinator, Crime Victim Compensation, and/or state or local

Victim/Witness Programs and provide reasonable assistance in contacting appropriate offices or coordinators involved in providing suitable services.

23.3.a.(5). Immediately notify the Resident Agents in Charge (RACs), who will in turn notify the SAC and the DCIS HQ VWAP Coordinator concerning actual instances of intimidation or harassment of any victim or witness and when a victim or witness requires protection against threats, harm, or intimidation.

23.3.b. **Field Management.** Field management, consisting of RACs, Assistant Special Agents in Charge (ASACs), and SACs will generally include providing special agents with sufficient guidance and resources to meet the requirements of this policy and coordinating with the HQ VWAP Coordinator, as needed. Additionally, RACs, through their ASACs and SACs, will be responsive to annual requests for victim information from the HQ VWAP Coordinator.

23.4. Victim and Witness Assistance

23.4.a. **Guidance.** All DCIS special agents engaged in the detection, investigation, or prosecution of crimes shall treat victims of and witnesses to crime with compassion, dignity, and courtesy and are mandated to assist them in obtaining medical, financial, or social services, if needed or requested. (b)(7)(E)

(b)(7)(E) However, all DCIS special agents must consider the guidance set forth in this chapter in those cases involving victims to which the law applies. DCIS special agents are required to identify victims of crime, notify them of their rights, and offer them services as described in this chapter. In the event a victim declines the services identified in this chapter, the agent should properly document the victim's informed declination of mandatory rights and services. DCIS is committed to providing crime victims and witnesses the rights and services required by the Directive and Instruction previously referenced. DCIS employees are expected to exercise sound judgment and discretion in deciding how best to accord victims and witnesses rights and services. When not prohibited by another statute, there is a presumption in favor of providing rather than withholding assistance and services to crime victims and witnesses.

23.4.b. **Victim's Rights.** Under the Crime Victims' Rights Act, 18 U.S.C. § 3771(c)(1), "Officers and employees of the Department of Justice and other departments and agencies of the United States engaged in the detection, investigation, or prosecution of crime shall make their best efforts to see that crime victims are notified of, and accorded, the rights described [below]." DCIS agents are expected to adhere to the victim's rights as listed in 18 U.S.C. § 3771(a) (outlined below) while conducting investigations for that department.

23.4.b.(1). The right to be reasonably protected from the accused.

23.4.b.(2). The right to reasonable, accurate, and timely notice of any public court proceeding, or any parole proceeding, involving the crime or of any release or escape of the accused.

23.4.b.(3). The right not to be excluded from any such public court proceeding, unless the court, after receiving clear and convincing evidence, determines that testimony by the victim would be materially altered if the victim heard other testimony at that proceeding.

23.4.b.(4). The right to be reasonably heard at any public proceeding in the district court involving release, plea, and sentencing; or any parole proceeding.

23.4.b.(5). The reasonable right to confer with the attorney for the Government in the case.

23.4.b.(6). The right to full and timely restitution as provided in law.

23.4.b.(7). The right to proceedings free from unreasonable delay.

23.4.b.(8). The right to be treated with fairness and with respect for the victim's dignity and privacy.

Victims of crimes investigated by DCIS 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.

23.5. Procedures. The following is a summary of the information and advisements DCIS special agents are to provide to crime victims and witnesses.

23.5.a. Provision of Brochure and Information. To comply with the requirements regarding victims' rights and the services to which they are entitled, special agents shall provide a DoD brochure (DD Form 2701) to victims and witnesses as soon as they are identified, unless such notification would jeopardize the investigation. Questions regarding assistance and services to victims and witnesses may be referred to the Victim Witness Coordinators at the cognizant U.S. Attorney's Office or the DCIS HQ VWAP Coordinator.

23.5.b. Victim Meeting Preparations–Services and Payments. Prior to meeting with a victim, agents should consider preparing for the meeting by taking the following steps and/or obtaining the following information:

23.5.b.(1). information relating to available emergency, medical, and social services (such as counseling and treatment programs) and how to obtain these services, if needed;

23.5.b.(2). information on restitution and compensation to which the victim may be entitled;

23.5.b.(3). information on victim counseling and treatment programs that may be available within the local community and assistance making contact with those services, if necessary;

23.5.b.(4). the availability of information regarding payment for testing and counseling in cases of sexual assaults and the payment of services for victims of domestic violence and stalking.

23.5.c. **Other Information/Coordination for Victims.** Other information and coordination by special agents for victims may include the following.

23.5.c.(1). An explanation of their rights as established under 18 U.S.C. §3771(a).

23.5.c.(2). An explanation of the role of the victim in a criminal investigation and prosecution and what may be expected from the criminal justice system and process, as well as the role of victims and witnesses.

23.5.c.(3). The protection from harassment and intimidation through the arrangement for victims and witnesses to receive reasonable protection from suspected offenders and persons acting in concert with or at the behest of the offender. Special agents should advise a victim or witness of their inability to provide for their safety. However, special agents can help the victim determine steps to be taken that will minimize the possibility of further harm from an offender. Section 23.7. includes more specific direction regarding threats to victims or witnesses.

23.5.c.(4). The return of property held as evidence.

23.5.c.(5). Notifications to victim's employers and creditors.

23.5.c.(6). Payment for forensic sexual assault examinations.

23.5.c.(7). Logistical information with regards to transportation, parking, childcare, translator services, and other investigation-related services.

23.5.c.(8). Programs for department employees who are victims of a crime (such as Employee Assistance Programs).

23.5.c.(9). Status updates (e.g., suspect arrest/apprehension, prosecution status) on the investigation in which they are involved. DCIS personnel should keep the victim informed of the case status to the extent possible as long as such information does not interfere with the investigation or jeopardize investigative steps or outcomes. While generally the responsibility of the trial counsel, a DCIS special agent will, if requested, inform victims and witnesses of the filing of charges against a subject, court appearances, and the release or detention, or pending action relating to the subject. The VRRRA (42 U.S.C. § 10607(c)(4)) further requires that a victim is provided a waiting area removed from and out of the sight and hearing of the defendant and defense witnesses during court proceedings.

23.5.c.(10). Preventing and/or avoiding disclosure of the name, address, telephone number, or any other contact or identifying information of victims and witnesses.

23.6. Victim Compensation and Expenditures. Compensation to victims may be provided by the state in which the crime occurs and is limited to the following that are not otherwise covered by insurance: medical or hospital bills, mental health counseling, actual loss of earnings due to crime-related injuries, loss of support for dependents of victims who are deceased or disabled as a result of crime, funeral and burial expenses, and loss or damage to eyeglasses, hearing aids, or other medically necessary devices. Also, in some states, victims may receive awards for pain and suffering.

23.6.a. **Statutory Protections.** Compensation and/or restitution to victims of crimes can also be ordered by the court. The Victim and Witness Protection Act provides for criminal and civil penalties/remedies against anyone who harasses, tampers with, or retaliates against a witness, victim, or informant. Restitution is not available through military court martial sentencing except through a pre-trial agreement. A military protection order or a civilian temporary restraining order can be obtained for the purpose of eliminating contact between suspects and witnesses or victims.

23.6.b. **Compensation by DCIS.** Only rare or unusual circumstances would require DCIS to compensate victims for the services obtained as a result of a crime, as described in section 23.4. Any considerations or requests for such funds must be coordinated with the DCIS HQ VWAP Coordinator through the RAC and/or the ASAC/SAC for the field office. No payments will be made to a victim without the authorization of the SAC, Internal Operations.

23.7. Victim/Witness Protection Procedures

23.7.a. **Temporary Protective Arrangements.** DCIS may take temporary protective arrangements to protect victims/witnesses whose continued cooperation/testimony is essential to a DCIS investigation. Such temporary arrangements are not intended to replace DOJ's Witness Security Program. Any protective arrangements undertaken by DCIS for a victim/witness not enrolled in the DOJ Witness Security Program require the approval of the Deputy Inspector General for Investigations. Special agents are not authorized to commit any funds for compensation and expenses of witnesses or Confidential Informants (CI), and are not authorized to make protective maintenance agreements. Additional information relating to CIs is included in SAM Chapter 7.

23.7.b. **Confidential Informant Protection Procedures.** Despite security measures to ensure the confidentiality and personal safety of witnesses (particularly those serving in a capacity as a CI), there will be occasions when a relationship with DCIS will be compromised. In some cases, it will become necessary for a CI to testify, thereby compromising the association with DCIS. The Victim and Witness Protection Act of 1982 (Public Law 97-291) and implementing DoD guidelines for the Act mandate that the Federal government do all that is possible within the limits of available resources to enhance and protect the necessary role of victims and witnesses in the criminal justice process. Occasionally, compromises of DCIS CIs or witnesses may lead to harassment or physical danger to the CI or family members, necessitating protection or a permanent relocation. These situations occur infrequently, but when they do, the DCIS office controlling the CI shall follow the procedures below.

(b)(7)(E)

23.8. Reporting Requirements. As required by DoD Directive 1030.01 and implemented by DoD Instruction 1030.2, the total number of victims and/or witnesses who receive DD Form 2071 will be collected at the end of each calendar year and reported annually by DCIS and each DoD criminal investigative organization. The DCIS HQ VWAP Coordinator will request statistical victim information from field offices and submit this information to the SAC, Internal Operations, who will subsequently provide this information to the DoD Legal Policy Office at the Pentagon by means of a DD Form 2076. The date the DD Form 2071 is given to the victim or witness constitutes the reportable date. This information should be recorded in a Form 1 and in the Case Reporting Information Management System (CRIMS).

23.9. Other Types of Victims

23.9.a. **Victim Advocates.** DCIS agents should also be aware of other types of victims, such as those who are children, incompetent, incapacitated, or deceased; and of the reporting requirements highlighted in the Attorney General Guidelines. 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) may be afforded rights similar to those of a victim:

- 23.9.a.(1). a spouse,
- 23.9.a.(2). a legal guardian,
- 23.9.a.(3). a parent,
- 23.9.a.(4). a child,
- 23.9.a.(5). a sibling,
- 23.9.a.(6). another family member,
- 23.9.a.(7). another person designated by the court.

See SAM Chapter 22 for additional information regarding juveniles.

23.9.b. **Child Abuse Victims and Reporting Requirements.** The Federal child abuse reporting law requires that when certain professionals (including law enforcement personnel, probation officers, criminal prosecutors, juvenile rehabilitation or detention facility employees, and social workers) working on Federal land or in a federally operated or contracted facility in which children are cared for or reside, learn facts that give reason to suspect that a child has suffered an incident of child abuse, shall as soon as possible make a report of the suspected abuse to an investigative agency designated by the Attorney General to receive and investigate such reports. State laws vary widely. Use of the standard written reporting form shall be encouraged, but its use shall not take the place of the immediate making of oral reports, telephonically or otherwise, when circumstances dictate. Reports should be documented as in any other investigative situation. Reports may be made anonymously. Reports are presumed to have been made in good faith and reporters are immune from civil and criminal liability arising from the report unless they act in bad faith. See 42 U.S.C. § 13031 and the AG Guidelines, Article III (L) for more information regarding these requirements.

23.9.c. **Victims of Identity Theft.** In addition to the victim's rights and services listed in this chapter, victims of identity theft should receive appropriate assistance for the unique circumstances of the crime. Assist victims of identity theft as follows.

23.9.c.(1). Refer victims to useful or relevant services specifically for victims of identity theft by other Federal agencies, including the Federal Trade Commission and non-Government organizations.

23.9.c.(2). Refer victims to relevant credit reporting services.

23.9.c.(3). Advise victims to file an individual police report.

ATTACHMENT A

ATTORNEY GENERAL GUIDELINES FOR VICTIM AND WITNESS ASSISTANCE



Attorney General Guidelines for Victim and Witness Assistance

2011 EDITION



U.S. Department of Justice
Office of Justice Programs
810 Seventh Street NW.
Washington, DC 20531

Eric H. Holder, Jr.
Attorney General

Laurie O. Robinson
Assistant Attorney General

Joye E. Frost
Acting Director, Office for Victims of Crime

Office of Justice Programs
Innovation • Partnerships • Safer Communities
www.ojp.usdoj.gov

Office for Victims of Crime
www.ovc.gov

NCJ 235121

October 2011

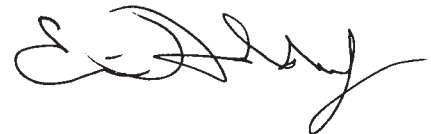


The Office of Justice Programs (OJP), headed by Assistant Attorney General Laurie O. Robinson, provides federal leadership in developing the Nation's capacity to prevent and control crime, administer justice, and assist victims. OJP has six components: the Bureau of Justice Assistance; the Bureau of Justice Statistics; the National Institute of Justice; the Office of Juvenile Justice and Delinquency Prevention; the Office for Victims of Crime; and the Office of Sex Offender Sentencing, Monitoring, Apprehending, Registering, and Tracking. More information about OJP can be found at <http://www.ojp.gov>.

FOREWORD

Our core mission is to pursue justice for criminal acts, and that pursuit includes justice for the victims of and witnesses to crime. Every day, Department personnel encounter individuals harmed by crime or who witnessed others being harmed by crime. How we treat those individuals has a huge impact on their confidence in the criminal justice system and their ability to heal and recover from crime. When the Department is successful in identifying and convicting offenders, our victim assistance efforts help victims navigate an unfamiliar system, foster accountability, and find affirmation for their suffering. In situations where the Department is unable to identify a perpetrator or bring a perpetrator to justice, our outreach and assistance can help victims access the services they need to recover and help them understand the criminal justice response.

For several decades, crime victims' laws have mandated that Department personnel provide victims with services and make our best efforts to see that victims are accorded their rights. To satisfy our statutory responsibilities, it is essential that Department personnel understand the legal mandates regarding victims and receive clear guidance about how to carry out those responsibilities. This updated edition of the *Attorney General Guidelines for Victim and Witness Assistance* reflects current statutory provisions, recognizes the technological and legal changes that have taken place since the previous Guidelines were promulgated, and incorporates best practices that will benefit victims and enhance investigations and prosecutions. It is my hope that this tool will enhance our ability to vindicate victims' rights and to provide victims with the services that they deserve.



Eric H. Holder, Jr.
Attorney General of the United States

[page intentionally left blank]

CONTENTS

Foreword	i
Article I: General Considerations	1
A. Statement of Purpose	1
B. How To Apply These Guidelines	1
Article II: Guidelines Applicable to All Components	3
A. Encouragement To Provide Services and Assistance.....	3
B. Victim Declinations of Services and Exercise of Rights	3
C. Privacy and Confidentiality Considerations for Victims and Witnesses	3
D. Mandatory Training	4
E. Mandatory Reporting of AG Guidelines Compliance.....	5
F. AG Guidelines Compliance Measures	5
G. Performance Appraisal	5
Article III: Who Is a Victim	7
A. Introduction	7
B. Victim Services Definition (VRRRA Definition)	7
C. Enforceable Victims' Rights Definition (CVRA Definition)	8
D. Harm	8
E. Other Persons Affected by a Crime	11
F. Culpability	11
G. Government Entities	12
H. Victims in a Foreign Country and Foreign Nationality Victims	12
I. Foreign Proceedings	13
J. Victims of Juvenile Offenders	13
K. Large Numbers of Victims	14
L. Particularly Vulnerable Victims	14
Article IV: Mandatory Services	25
A. Background.....	25
B. Responsible Officials	25
C. Timing of Services.....	26
D. Coordination of Services.....	26

E. Victim Identification	27
F. Reasonable Protection	27
G. General Information	28
H. Services Referrals.....	29
I. Notice of Case Events	30
J. Separate Waiting Area.....	32
K. Return of Property	32
L. Employer/Debt Notification.....	33
Article V: Victims’ Rights Under the CVRA	35
A. Background.....	35
B. Responsibilities of Department Personnel.....	35
C. Right to Reasonable Protection.....	37
D. Right to Reasonable, Accurate, and Timely Notice	37
E. Right Not To Be Excluded From Court	39
F. Right To Be Reasonably Heard.....	40
G. Reasonable Right To Confer With the Prosecutor	41
H. Right to Full and Timely Restitution as Provided in Law	42
I. Right to Proceedings Free From Unreasonable Delay	47
J. Right to Fairness and Respect for Dignity and Privacy	47
K. In-Court Enforcement Mechanisms	48
Article VI: Witnesses	51
A. Victims’ Services and Rights Laws Do Not Cover Witnesses.....	51
B. Witness Security	51
C. Logistical Assistance	52
D. Notification of Offender Release	52
Article VII: Non-Litigability	53
Appendixes	55
A. Victims’ Rights and Restitution Act	55
B. Crime Victims’ Rights Act	59

ARTICLE I

GENERAL CONSIDERATIONS

A. Statement of Purpose

The purpose of this document, the *Attorney General Guidelines for Victim and Witness Assistance* (AG Guidelines), is to establish guidelines to be followed by officers and employees of the U.S. Department of Justice (Department) investigative, prosecutorial, correctional, and parole components in the treatment of victims of and witnesses to crime. In 1982, Congress directed the Attorney General to promulgate the first AG Guidelines, which have been revised periodically to reflect changes in the law. (See 18 U.S.C. § 1512 note (1984) (Federal Guidelines for Treatment of Crime Victims and Witnesses in the Criminal Justice System)).

These AG Guidelines supersede the *Attorney General Guidelines for Victim and Witness Assistance* (2005 ed.).

B. How To Apply These Guidelines

1. Underlying Authorities

Federal victims' services and rights laws are the foundation for the AG Guidelines. The core statutes are the Victims' Rights and Restitution Act (VRRRA), 42 U.S.C. § 10607 (2006) (containing mandatory services), and the Crime Victims' Rights Act (CVRA), 18 U.S.C. § 3771 (2006 & Supp. III 2009) (containing court enforceable rights), but additional rights and requirements exist in other statutes and rules of criminal procedure. In the text of the AG Guidelines, all statutory requirements or rules of criminal procedure are followed by a direct citation to the applicable statute or rule. Guidelines that are purely Department policy, as opposed to statutory law, will not be followed by a citation. Guidelines that are policy intended to implement a statutory right, provision, or procedural rule will be followed by a citation referring to the statute or rule.

2. Obligation Definitions

The AG Guidelines use the word "shall" where "shall" appears in a statute or when the policy is mandatory. The use of the term "shall" means that the relevant guideline is mandatory, though room may remain for individual judgment in determining how best to comply with the guideline. When the AG Guidelines use the word "should," personnel are expected to take the action or provide the service described unless there is an appropriate, articulable reason not to do so. When the AG Guidelines use the word "may," personnel are permitted to use their discretion about whether and how to provide assistance. Other language may be used in the AG Guidelines to describe the obligations of personnel; phrases such as "are encouraged" or "make reasonable efforts" are intended to have their usual and customary meaning.

3. Coverage

The AG Guidelines apply to all personnel in the Department who are engaged in or support investigative, prosecutorial, correctional, or parole functions within the criminal justice system. They apply to staff regardless of title, grade, or job description who have contact with victims or take actions that impact victims. Department managers should require all contractors whose employees come into contact with crime victims to provide employee training on AG Guidelines compliance. Department components should encourage non-Department personnel specially assigned or deputized to work with Department components to learn and comply with federal victims' services and rights laws and the AG Guidelines.

The AG Guidelines are intended to serve as a model for guidelines on the fair treatment of crime victims and witnesses for other state and federal law enforcement agencies.

4. Organization

The AG Guidelines are organized around the two primary crime victims' services and rights laws. Articles I and II deal with general policies affecting all components and victims. Article III contains the basic definitions of victim under both of the key laws, as well as sections on unique victim populations. Article IV covers the Department's mandatory obligations to provide services to victims of a crime under the VRRRA. Article V covers the CVRA provisions that victims of a charged offense can enforce during a prosecution. Article VI addresses witnesses only. Article VII consists of the Department's statement on non-litigability.

ARTICLE II

GUIDELINES APPLICABLE TO ALL COMPONENTS

A. Encouragement To Provide Services and Assistance

A strong presumption exists in favor of providing, rather than withholding, assistance and services to victims of crime. Federal statutes define mandatory services and court-enforceable rights for federal crime victims that establish a minimum baseline for the Department's obligation to crime victims. Department personnel are encouraged to provide additional assistance to crime victims where appropriate and within available resources, as situations warrant.

B. Victim Declinations of Services and Exercise of Rights

Department personnel are required by law and under the AG Guidelines to identify victims of a crime, notify them of their rights, and offer them services as described in the AG Guidelines. Victims, however, are not required to exercise their rights or to accept these services and may choose at any point in the criminal justice process to decline to receive further services or exercise their rights. Department personnel need not provide services or support the exercise of rights that victims have made an informed decision to decline. When a victim declines to receive services or to exercise rights, Department personnel should attempt to ascertain whether the victim wants to decline all future services and the exercise of all rights or only one or more specific service or right. In the latter case, Department personnel should continue to provide services and support the exercise of rights that have not been declined. The employee should consider documenting the victim's informed declination of mandatory services and the exercise of rights.

C. Privacy and Confidentiality Considerations for Victims and Witnesses

1. Private Information

Department personnel engaged in the investigation or prosecution of a crime shall be mindful of the privacy concerns of victims and witnesses. In particular, Department personnel should use their best efforts to protect private information by redacting this information from records or documents that will be placed in the public record, unless specifically required by court rules or procedure. (*See, e.g., Fed. R. Crim. P. 49.1*). Private information includes Social Security numbers, bank account information, dates of birth, and, in some circumstances, may include an individual's identity, address, contact information, or location.

Department personnel should seek protective orders or employ other means when necessary to safeguard private information from becoming public or from being used in proceedings if the information is not relevant. If private information must be disclosed

in proceedings or in the course of discovery, Department personnel should seek protective orders to prevent dissemination of this information outside of the proceedings. (*See also* Fed. R. Crim. P. 17(c)(3)).

2. Sharing of Information for Law Enforcement Purposes

Although private information should be safeguarded from public disclosure, when necessary, information may be shared among investigative, prosecutorial, corrections, and parole agencies, and with the court or defense. Department personnel directly involved with providing victim and witness assistance should therefore inform victims and witnesses that private information will likely be shared among Department components or may be shared with other law enforcement entities as appropriate, may be shared with the court, or may have to be provided to the defense during the course of discovery. If the victim or witness raises concerns regarding the disclosure of such information that are warranted, Department personnel should employ their best efforts to protect this information from disclosure, or if such a disclosure is required, employ their best efforts to address appropriate and necessary concerns for victims and witnesses.

3. Dissemination of Private Information to the Media or Public

Department personnel should use their best efforts to refrain from releasing personal or confidential information about victims and witnesses to the press or public. Personal or confidential information in this context may include the individual's name, address, contact information, identifying information, or other information or material that may allude to the identity of the victim or witness. Moreover, Department personnel should refrain from making any public statements that concern the identity, testimony, or credibility of any prospective witness. (Release of Information by Personnel of the Department of Justice Relating to Criminal and Civil Proceedings, 28 C.F.R. § 50.2(b)(6)(iv) (2010)).

In addition, Department personnel receiving requests for information about a case or matter should be mindful that information generally subject to release under the Privacy Act of 1974 (Privacy Act), 5 U.S.C.A. § 552a (West 2010), or the Freedom of Information Act (FOIA), 5 U.S.C. § 552 (2006 & Supp. III 2009), may otherwise be protected from disclosure by virtue of the privacy considerations due to victims under the CVRA. (*See* Article V.J.).

D. Mandatory Training

All Department personnel whose primary job responsibilities affect crime victims and witnesses shall have access to the AG Guidelines and complete a basic training session about the AG Guidelines, and statutory victims' services and rights, within a reasonable time after implementation of the AG Guidelines 2011 edition. Thereafter, all such employees shall receive the same access and training within a reasonable amount of time after assuming primary job responsibilities that impact crime victims and witnesses. Components should provide additional training on victim-related topics as necessary.

COMMENTARY

Components are encouraged to develop training in addition to the mandatory training required by this guideline. Such training can be more frequent, as with an annual or biannual basic training requirement, or can be tailored to specific job responsibilities or frequency of victim contact.

At the discretion of the component, Department personnel whose primary responsibilities are for civil cases and litigation may be exempted from this training requirement. If exempting personnel from the training, components should be mindful that some civil cases will have the potential to directly or indirectly affect crime victims, and personnel assigned to such cases should have at least a rudimentary understanding of the Department's obligations to victims.

E. Mandatory Reporting of AG Guidelines Compliance

The Director of the Office for Victims of Crime (OVC) has the statutory responsibility for monitoring Department compliance with the AG Guidelines. (42 U.S.C. § 10603(c)(3)(A) (2006 & Supp. III 2009)). Components shall report to the Attorney General, through the OVC Director, about their compliance by means of an Annual Compliance Report containing the relevant data (including the numbers of crime victims offered services) requested by the OVC Director. Unless directed otherwise by OVC, a component's Annual Compliance Report shall be submitted to OVC no later than April 20 of the fiscal year following the fiscal year that is the subject of the report.

F. AG Guidelines Compliance Measures

Each component shall devise and implement performance measures that will ensure component compliance with the AG Guidelines and the statutes upon which they are based. Implementation of compliance measures should be included in the component's Annual Compliance Report.

G. Performance Appraisal

The annual work plans and performance appraisals of each appropriate federal law enforcement officer, supervisor, investigator, prosecutor, corrections officer, and parole official (and appropriate staff of those agencies) shall encompass, as a required activity, implementation and evaluation of adherence or nonadherence with the victims' rights and victims' and witnesses' services provisions set forth in the AG Guidelines. All investigative, prosecutorial, correctional, and post-correctional components with responsibilities for providing rights and services to victims should include the discharge of such responsibilities among those components' criteria for reviews and evaluations. Verification of the institution of this recommendation must be included in the Annual Compliance Report.

ARTICLE III

WHO IS A VICTIM

A. Introduction

Determining who qualifies as a victim may be one of the most difficult aspects of providing victim assistance. Federal statutes typically contain victim definitions applicable only to a particular statute's provisions. Two statutes describe the majority of the Department's responsibilities to crime victims. The first, the VRRRA, mandates services to those directly harmed by a crime, while the CVRA establishes court-enforceable rights for those who are directly and proximately harmed by a charged offense. There are also separate victim definitions and unique requirements for particular types of victimization.

B. Victim Services Definition (VRRRA Definition)

1. **Basic Definition:** For purposes of providing the services described in Article IV of these AG Guidelines, a victim is "a person that has suffered direct physical, emotional, or pecuniary harm as a result of the commission of a crime. . . ." (42 U.S.C. § 10607(e)(2)(A)).
2. **Institutional Victims:** If a victim is an institutional entity, services should be provided to an authorized representative of the entity. (42 U.S.C. § 10607(e)(2)).
3. **Representative Victims:** If a victim is under 18 years of age, incompetent, incapacitated, or deceased, services should be provided to one of the following (in order of preference): a spouse, legal guardian, parent, child, sibling, another family member, or another person designated by the court. (42 U.S.C. § 10607(e)(2)(B)). An incapacitated victim is any victim who is unable to interact with Department personnel for the purpose of receiving services as a result of a cognitive impairment or other physical limitation, or because of physical restraint or disappearance. More than one representative victim can be identified and provided with services depending upon the circumstances. It is Department policy that under no circumstances shall a person culpable for the crime be treated as a representative victim.
4. **Timing:** Department responsibilities to crime victims begin as soon as possible after the detection of a crime at which they may be undertaken without interfering in the investigation. (42 U.S.C. § 10607(b)). Generally, this point in time is defined by the opening of a criminal investigation.

In some situations, an investigation may be initiated at a point in time when it is still unclear whether a crime was committed. In those situations, personnel should follow the guidance of Article II.A.

The end point for Department services obligations may be difficult to determine, and personnel should use their discretion and sound judgment to assess whether an investigation or prosecution is finally concluded. At that point, Department personnel may continue to provide services to the extent permitted by law and with available resources.

C. Enforceable Victims' Rights Definition (CVRA Definition)

1. **Basic Definition:** For purposes of enforcing the rights discussed in Article V, a victim is “a person directly and proximately harmed as a result of the commission of a Federal offense or an offense in the District of Columbia” (18 U.S.C. § 3771(e)) if the offense is charged in federal district court or the Superior Court of the District of Columbia.
2. **Institutional Victims:** A victim may be a corporation, company, association, firm, partnership, society, or joint stock company. (*See* 1 U.S.C. § 1 (2006)).
3. **Representative Victims:** If a victim is under 18 years of age, incompetent, incapacitated, or deceased, a family member or legal guardian of the victim, a representative of the victim's estate or any other person so appointed by the court may exercise the victim's rights, but, in no event, shall the defendant serve as a guardian or representative for this purpose. (18 U.S.C. § 3771(e)). An incapacitated victim is any victim who is unable to interact with Department personnel as a result of a cognitive impairment or other physical limitation, or because of physical restraint or disappearance.
4. **Timing:** CVRA rights attach when criminal proceedings are initiated by complaint, information, or indictment. If the defendant is convicted, CVRA rights continue until criminal proceedings have ended. For example, CVRA rights continue through any period of incarceration and any term of supervised release, probation, community correction, alternatives to incarceration, or parole. Absent a conviction, a victim's CVRA rights cease when charges pertaining to that victim are dismissed either voluntarily or on the merits, or if the government declines to bring formal charges after filing a complaint.
5. **Scope of the Offense:** Because the particular charges filed in a case will define the group of individuals with CVRA rights, prosecutors should carefully consider the scope of the charged offense when crafting the charging document. Charging decisions are within the discretion of the prosecution, and an individual can qualify as a CVRA victim regardless of whether he or she is named in the indictment. In cases with CVRA victims, prosecutors should give consideration to CVRA compliance from the outset of the prosecution through its conclusion.

D. Harm

1. **Direct and Proximate Harm**

Determining whether a person meets the harm element of the legal definition of victim under the VRRRA or CVRA requires a fact-specific analysis of both the nature of the harm allegedly suffered by the person and the crime that is alleged to have caused the harm. To qualify as a victim, both statutes require the alleged harm must be a direct

consequence of the crime; that is, the harm must generally be a “but for” consequence of the conduct that constitutes the crime, specifically the crime under investigation, that has been charged, or for which there has been a conviction, depending on the stage of the criminal justice process. Intervening or contributing actions of the person suffering harm, or of a third party, may preclude a determination that the crimes being investigated or the offense charged directly caused the harm.

The CVRA requires an additional showing that the alleged harm must have been proximately caused by the offense. This showing ordinarily requires that the alleged harm must have been a reasonably foreseeable result of the charged offense. If both conditions are met, the person at issue meets the CVRA harm element.

COMMENTARY

Children who are depicted in child pornography that has been advertised, transported, distributed, received, accessed, or possessed are presumed to have been directly and proximately harmed as a result of those crimes for purposes of determining whether they are a victim under the VRRRA or CVRA.

There may be instances in which case law developed in other legal contexts should be considered when determining issues of direct and proximate harm. For example, jurisprudence concerning direct versus indirect purchasers, as well as subject matter jurisdiction, under the antitrust laws is relevant to the issue of when a person injured by an antitrust violation has suffered the requisite harm under the VRRRA and the CVRA.

There may also be instances in cases involving tax administration or other financial crimes in which a person, not charged with an offense, suffers harm due in part to their own willful participation in a scheme or transaction. Knowing and willful participation in such a scheme or transaction generally negates a determination of direct harm from the financial crimes being investigated or offense charged.

2. Types of Harm

The harm can be physical, emotional, or pecuniary. In the absence of physical or pecuniary harm, emotional harm may be presumed in violent crime cases where the individual was actually present during a crime of violence, or, if not present, received information about a violent act attempted against him or her. In all other cases, emotional harm should not be presumed in the absence of physical or pecuniary harm, but rather the existence of cognizable emotional harm should be determined on a factual, case-by-case basis.

COMMENTARY

The impact of witnessing traumatic events involving loss of life and violent injury – along with the belief that one’s own life will be taken – cannot be understated. Emotional injury may result in a range of physiological and psychological reactions, from temporary impairment in the ability of victims to cope and function to acute stress reactions and post-traumatic stress disorder. Visual imagery related to the event and the emotional and physical reactions associated with reliving the experience may remain with victims for many

COMMENTARY (CONTINUED)

years. The role of victim assistance personnel in investigative agencies is particularly critical to ensuring victims who suffer emotional injury receive timely intervention, information, and referrals. Later, criminal justice proceedings may reopen emotional wounds, and timely and appropriate assistance from prosecution-based victim assistance personnel can help meet victims' needs at this critical stage. In situations involving victims under 18 years of age who may have suffered emotional injury, victim assistance personnel will need to involve a parent or guardian in the provision of appropriate services.

In cases involving tax administration or other financial crimes, such as a tax shelter investigation, harm should not be presumed merely because participants paid a fee to the promoter for participation or for some fraudulent benefit promised but not received. In such cases, a determination that a participant suffered harm should be based on all of the facts and circumstances. For additional guidance, contact the Tax Division.

3. Harm in Identity Theft Cases

Determining harm in identity theft cases can be particularly difficult. Where Department personnel discover that a suspect possesses an individual's personally identifying information (PII), personnel should determine, based on the facts known at the time and any reasonable additional investigation, whether the PII was used in a way that could cause harm to the individual. If no evidence indicates that the information was misused, there is likely no direct harm to support victim status. If resources permit, Department personnel may notify such individuals that their information was compromised to allow the individuals to take appropriate measures to protect their credit.

If it appears that an individual's PII was used by the suspect or others in committing a crime, Department personnel should determine whether the individual suffered direct harm as a result of the misuse. Direct harm in these situations is usually pecuniary and may include out-of-pocket losses as well as time reasonably spent in an attempt to remediate actual or intended harm. In extraordinary cases, there may be solely or primarily emotional harm, such as harm to reputation from a false arrest that is a direct result of the misuse, with negligible or no pecuniary harm. Department personnel should consider the nature and extent of emotional harm when evaluating whether an individual should be classified as a victim for purposes of victims' rights and services.

In a large data breach case, the suspect or suspects may obtain PII for thousands or even millions of individuals. If there is no indication from the facts known at the time and any reasonable additional investigation that the information has been misused, then the direct harm may only be to the entity that legitimately held the PII. That entity may have suffered pecuniary harm as a result of having to respond to the data breach, and, if so, would fall within the definition of victim for the purposes of obtaining victim services and exercising victim rights (unless it is a governmental entity and therefore outside the definition of victim (*see* Article III.G.)). In such situations, state laws or civil court orders may obligate the entity to inform the individuals whose information was compromised so that they may take any action they deem appropriate to protect their credit.

Department personnel should encourage entities to notify individuals, with or without legal mandates, or, if resources permit, take steps themselves to notify such individuals that their information was compromised to allow the individuals to take appropriate measures to protect their credit.

E. Other Persons Affected by a Crime

In some cases there may be persons who do not fall under any statutory definition of crime victim but who nevertheless are affected by the criminal justice process concerning a defendant. Department personnel may provide such persons with appropriate assistance within available resources. To the extent permitted by law, and consistent with the interests of the United States in a particular case, persons who do not fit the CVRA definition of crime victim may be accommodated in their desire to participate in court proceedings or obtain information about the prosecution.

COMMENTARY

Examples of such persons include, but are not limited to, the following:

In a prosecution of a felon in possession of a firearm, a person known to Department personnel to have a credible reason to fear the defendant's gun possession, such as a known domestic violence victim who had been threatened with harm by the defendant, may be provided with assistance in connection with the possessory crime prosecution.

In a prosecution for immigration fraud based on misrepresentations about participation in the torture of others, witnesses testifying that the defendant had perpetrated torture upon them may be provided with assistance in connection with the immigration fraud prosecution.

F. Culpability

A person who is culpable for or accused of the crime being investigated or prosecuted should not be considered a victim for purposes of the rights and services described in the AG Guidelines. The determination of whether a person is culpable should be based on the facts and circumstances known at the time of investigation, prosecution, or post-conviction, and should be reevaluated as additional facts and circumstances become known. A person who may be culpable for violations or crimes other than the crime being investigated or prosecuted may be considered a victim under this policy in some circumstances.

Inmates who are victims of crime during their incarceration for other offenses may be considered victims. An inmate's detention, however, may prevent the inmate from exercising the rights and receiving the services normally afforded to victims. For example, Department personnel are not required by the AG Guidelines to transport inmates to court to attend hearings relating to crimes against those inmates.

COMMENTARY

Victims of involuntary servitude or trafficking may be considered victims for purposes of the prosecution of those crimes despite any legal culpability that the victims may have for ancillary offenses, such as immigration or prostitution crimes. A witness who is threatened or injured as the result of an attempt by another person to prevent the witness from cooperating with law enforcement or testifying before a grand jury or in court should be treated as a victim of the intimidation crime even though the witness may have some culpability in the matter about which he or she was testifying.

In contrast, individuals who are knowing and willful participants in an illegal tax shelter or other financial fraud are generally not considered victims of the crimes charged against the shelter or fraud promoters, even when the individuals are not criminally culpable for the charged crimes or any of the crimes under investigation. See Article III.D's commentary discussion regarding willful participation in a fraudulent scheme.

G. Government Entities

Neither the federal government nor any state, local, tribal, or foreign government or agency thereof fall under the definition of crime victim for either mandatory services or court-enforceable rights; however, they may qualify for restitution under federal restitution statutes. *See* 18 U.S.C. § 3664(i) (2006 & Supp. II 2008). Department personnel in their discretion may provide assistance to these entities pursuant to the policy contained in section E of this Article. Nothing herein is intended to prevent a government employee from asserting rights or receiving services as a victim of crime, even if such crime against the employee arose out of that employee's duties.

H. Victims in a Foreign Country and Foreign Nationality Victims

The victims' services and rights laws apply to foreign nationals meeting the definitions of victim under the VRRRA and CVRA, regardless of whether they reside in the United States. Each country has its own procedures and requirements for contacting persons located in its territory. Due to sovereignty concerns, many countries limit or prohibit foreign government officials from directly contacting persons within that country's borders. Therefore, contact with victims and witnesses residing in other countries, for any purpose, needs to be coordinated with the appropriate officials of the host government through either the Department's Office of International Affairs (OIA) or the United States investigative attaché in the country where the victim resides. If victims in other countries do not have the ability to speak or read English, Department personnel should arrange for written communications to be translated. Because the coordination process can take several weeks, Department personnel should allow for extra time to notify victims in foreign countries. In cases with large numbers of victims, where Department personnel are using alternate means of notification, such as publication notice through media outlets or on a public Web site, coordination with an investigative attaché or OIA might not be necessary unless using a foreign media outlet or entity.

There are various types of immigration relief available to victims or witnesses who assist in the investigation or prosecution of certain criminal activity. Department personnel shall not offer victims or witnesses legal advice about immigration relief issues. If a victim or

witness is pursuing legal status, Department personnel should provide, when warranted by the circumstances, the supporting documentation that must come from law enforcement.

Department personnel should inform the prosecutor immediately about any immigration relief issues in the case. Department personnel should be aware that immigration relief may constitute a benefit to the victim or witness, and this benefit may be subject to disclosure if the victim or witness testifies at trial.

COMMENTARY

Department personnel seeking to fulfill victim notification responsibilities should consult the OIA attorney responsible for handling matters in the country where the victim resides to obtain guidance and approval for appropriate victim notification procedures. In addition, Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), or other investigative agency attaché stationed abroad, and assigned to United States Embassies in countries with which the United States has diplomatic relations, may have information regarding appropriate notification procedures for victims residing in those countries.

Immigration relief for victims or witnesses may include an S–5 visa, U visa, or T visa. See S–5 visa (8 U.S.C. § 1101(a)(15)(S) (2006 & Supp. III 2009)); U visa (8 U.S.C. §§ 1101(a)(15)(U), 1184(p), 1255(l)); and, T visa (8 U.S.C. § 1101(a)(15)(T)).

I. Foreign Proceedings

Some crimes perpetrated in foreign countries or by persons located in foreign countries are also subject to United States jurisdiction. When a crime being investigated or prosecuted in the United States is also the subject of a foreign investigation or prosecution, victims in the United States investigation/prosecution may need assistance in obtaining information about and participating in the foreign prosecution. Department personnel may assist victims in the United States investigation/prosecution with information about foreign prosecutions and facilitate participation therein when appropriate and feasible with available resources.

J. Victims of Juvenile Offenders

Generally, victims of juvenile offenders are victims for purposes of the VRRRA, CVRA, and the AG Guidelines, but the Federal Juvenile Delinquency Act (FJDA) (18 U.S.C. §§ 5031–5042 (2006)) restricts the type of information that may be disclosed to victims about investigations and proceedings regarding juvenile offenders unless the juvenile waives the restrictions or has been transferred for criminal prosecution as an adult. This law limits the statutory CVRA rights normally provided to victims.

1. Victim Services

During the investigative stage, a crime victim should receive the services to which the victim would normally be entitled, but only a general statement about the progress of an investigation into the role of a juvenile suspect may be disclosed. Investigators and other Department personnel are cautioned that the name and other identifying data about a suspect who is known or believed to have been younger than 18 when the crime occurred should not be disclosed.

2. Victim Rights Available in Juvenile Cases

In federal juvenile delinquency proceedings, the FJDA nondisclosure provisions circumscribe victims' ability to exercise many CVRA rights. (*Compare* 18 U.S.C. § 3771(a)(2)-(4) *with* 18 U.S.C. § 5038(a)). Nonetheless, victims can, as in other criminal cases, be offered reasonable protection when needed (18 U.S.C. § 3771(a)(1)); confer with the attorney for the government (18 U.S.C. § 3771(a)(5)); and make known their injuries and views on appropriate disposition including whether the prosecutor should move to detain, dismiss, defer prosecution, move to transfer to adult status or accept a plea, and how severe a sentence is warranted. Prosecutors should inform victims that presentence reports and victim impact statements are not mandated at dispositional hearings but that a victim may prepare such a statement for the prosecutor to offer to the court. The prosecutor may also request that the court order the probation office to prepare a victim impact statement. Victims may be entitled to full and timely restitution (18 U.S.C. § 3771(a)(6); 18 U.S.C. § 5037(a)), and have the right to be treated with fairness and respect for their dignity and privacy (18 U.S.C. § 3771(a)(8)). Prosecutors shall advise victims that they can seek the advice of a private attorney. (18 U.S.C. § 3771(c)(2)). Prosecutors are not permitted to convey to the victim any prosecutorial information about the progress of a juvenile proceeding unless the court makes a delinquency finding. After a finding of delinquency, federal law explicitly permits disclosure, on request, of information about the final disposition to the victim or, if the victim is deceased, to the victim's immediate family. (18 U.S.C. § 5038(a)(6)). Upon request, a victim should be apprised of the final disposition of the case and the sentence imposed on the offender, but not the date when the juvenile offender in his or her case will be released from custody, unless the victim has requested such notification at that time.

K. Large Numbers of Victims

Cases with a large number of victims present unique challenges in affording victims' rights and services. While individual contact with victims is preferred, such contact may not be feasible as the number of victims grows into the hundreds and thousands. Department personnel should use new technology and be creative, with the goal of providing rights and services to the greatest extent possible given the circumstances and resources available. (*See* specific discussions in Article IV.E. (victim identification), V.D.2. (right to notice), V.E.4. (right not to be excluded from court), V.F. (right to be reasonably heard), and V.G.3. (right to confer)).

L. Particularly Vulnerable Victims

1. Child Victims

a. Department Obligations

- (1) Department personnel should be aware of any obligations under applicable state, tribal, and federal law to report suspected child abuse.

- (2) Department personnel should be aware that there are many statutory protections for child victims and witnesses. More extensive guidance about these protections and other promising practices are contained in other Departmental resources. Department personnel working on cases involving child victims and witnesses should review and become familiar with the protections contained in 18 U.S.C. § 3509 (2006 & Supp. III 2009) and other Department resources dealing with child victims and witnesses.
- (3) Department personnel should be aware of the trauma that child victims and witnesses may experience when they are asked to relive the crime during the investigation and prosecution of a criminal case, particularly when testifying in court. A primary goal of Department personnel, therefore, shall be to reduce the potential trauma to child victims and witnesses that may result from their contact with the criminal justice system. To that end, Department personnel are required to provide age-appropriate support services to these victims, and referrals for community-based services to parents and guardians as indicated. (*See Article IV.H.*).

b. Definitions

- (1) Child: For purposes of the AG Guidelines, a child is a person under the age of 18 years. For guidance on notifying child victims after they reach the age of majority, *see Article IV.I.5.*
- (2) Child Abuse: For the purposes of this section, “child abuse” means the physical or mental injury, sexual abuse or sexual exploitation, or negligent treatment of a child. “Sexual abuse” includes rape, molestation, or incest with children. “Sexual exploitation” includes the production, distribution, receipt, possession, or access of child pornography, as well as the commercial sexual exploitation of children (prostitution), and the employment, use, persuasion, inducement, enticement, or coercion of a child to engage in, or assist another person to engage in, sexual abuse or sexual exploitation of children. The term “negligent treatment” means the failure to provide, for reasons other than poverty, adequate food, clothing, shelter, or medical care so as to seriously endanger the physical health of the child. “The term ‘child abuse’ does not include discipline administered by a parent or legal guardian to his or her child provided it is reasonable in manner and moderate in degree and otherwise does not constitute cruelty.” (42 U.S.C. § 13031(c)(8) (2006)).

c. Child Abuse Reporting Requirements

(1) Report Suspected Child Abuse

Department personnel should promptly report suspected child abuse to a person designated to receive such reports in each office. This requirement is in addition to, not in place of, mandatory reporting requirements under state, tribal, and federal law with which Department personnel shall also comply.

(2) State Mandatory Reporting Laws

All Department personnel should refer to their state child abuse reporting laws to determine the scope of the obligation in cases of suspected child abuse. State laws vary substantially. Some states require mandatory reporting of child abuse or neglect by all persons within their boundaries; others require such reporting only from individuals engaged in expressly listed occupations. A report should be made even if the information inadvertently comes to the employee's attention, but not if the suspected child abuse has already been reported and is the subject of an existing report or investigation. Reports of child abuse required by state or local law shall be made to the agency or entity identified in accordance with that law.

(3) Federal Reporting Requirement

(a) Mandated Reporters

The federal child abuse reporting law requires certain professionals (including law enforcement personnel, probation officers, criminal prosecutors, juvenile rehabilitation or detention facility employees, and social workers) working on federal land or in a federally operated (or contracted) facility in which children are cared for or reside, to report suspected child abuse to an investigative agency designated by the Attorney General to receive and investigate such reports. (42 U.S.C. § 13031(a)).

(b) Sanctions for Failure To Report

A covered professional who, while working on federal land or in a federally operated (or contracted) facility in which children are cared for or reside, learns of facts that give reason to suspect that a child has suffered an incident of child abuse and fails to timely report shall be fined or imprisoned not more than one year or both. (18 U.S.C. § 2258 (2006)).

(c) Agencies Designated by the Attorney General To Receive Reports

Reports of child abuse on federal lands or in federally operated (or contracted) facilities pursuant to 42 U.S.C. § 13031 shall be made to the local law enforcement agency or local child protective services agency that has jurisdiction to investigate reports of child abuse or to protect child abuse victims in the area or facility in question. When no such agency has entered into a formal written agreement with the Attorney General to investigate such reports, the FBI shall receive and investigate such reports. (28 C.F.R. § 81.3 (2010)).

(4) Reporting Child Abuse in Indian Country

Reporting child abuse in Indian Country is governed by 18 U.S.C. § 1169 (2006) and 25 U.S.C. § 3203 (2006). Covered professionals shall report suspected cases of child abuse to the federal, state, or tribal agency with primary responsibility

for child protection or investigation of child abuse within the portion of Indian Country involved. If the report involves a potential crime and either involves an Indian child or an Indian suspect, the local law enforcement agency is required to make an immediate report to the FBI. (25 U.S.C. § 3203(b)(2)).

(5) Immediate Reports

The report of suspected child abuse should be made by a method best suited to giving immediate notice. According to 42 U.S.C. § 13031(e), use of a standardized form is encouraged, but shall not take the place of the immediate making of reports by other means when circumstances dictate. Reports may be made anonymously. Reports are presumed to have been made in good faith and reporters are immune from civil and criminal liability arising from the report unless they act in bad faith. (42 U.S.C. § 13031(f)). Reporters should document their report in the same manner that they document other important work-related actions.

(6) Child Abuse Discovered From a Confidential Source or Investigation

When Department personnel suspect that a child is being abused based on information gathered during a confidential investigation or from a confidential source, they should make every effort to report the abuse to the appropriate authorities in order to protect the safety of the child. If it is not possible to report the suspected child abuse without significantly compromising the investigation or other confidential source such as classified information, or endangering public safety, Department personnel shall obtain guidance from the designated component responsible official. (*See* Article IV.B. for a listing of component responsible officials). The component responsible official shall not delegate this responsibility. Component responsible officials are encouraged to consult personnel with expertise in the subject matter of child abuse and should be aware of the penalties, some of them criminal, that could result from a decision not to report.

d. Privacy Protections for Child Victims and Witnesses

Department personnel should scrupulously protect children's privacy in accordance with 18 U.S.C. § 3509(d), the AG Guidelines, and other Departmental policies. A child's name or other identifying information (other than initials or an alias) should not be reflected in court documents or other public records unless otherwise required by law.

(1) Motion To Render Nonphysical Identifying Information Inadmissible

Federal prosecutors may move in any prosecution under Chapter 110 or section 1466A of title 18 for an order that the name, address, Social Security number, and other nonphysical identifying information (other than the age or approximate age) of any minor who is depicted in any child pornography shall not be admissible and may be redacted from otherwise admissible evidence. (18 U.S.C. § 2252A(e)) (2006 & Supp. III 2009).

(2) Sanctions for Violating the Disclosure Rules

A knowing or intentional violation of the privacy protection accorded children in 18 U.S.C. § 3509(d) is a criminal contempt punishable by not more than one year's imprisonment, or fine, or both. (18 U.S.C. § 403 (2006)).

e. Child Protections During Criminal Investigations

(1) Multidisciplinary Child Abuse Teams

A multidisciplinary child abuse team is a professional unit composed of representatives from health, social service, law enforcement, and legal service agencies to coordinate the assistance needed to handle cases of child abuse. (18 U.S.C. § 3509(a)(7)). The goals of the multidisciplinary team are (1) to minimize the number of interviews to which the child is subjected to reduce the risk of suggestibility in the interviewing process, (2) to provide needed services to the child, and (3) to monitor the child's safety and well-being.

A multidisciplinary child abuse team shall be used when feasible. (18 U.S.C. § 3509(g)(1)). Department personnel should use existing multidisciplinary teams in their local communities. Law enforcement personnel are encouraged to bring other professionals onto the teams. Local laws and guidelines concerning the teams may vary, and federal personnel should become familiar with the local provisions. If no multidisciplinary team is in place in a particular community, Department personnel should coordinate with the local Child Protective Services and other agencies and experts to assemble the expertise necessary to ensure the most effective response to the crime and victim.

(2) Investigation/Forensic Interviewing of Child Victims and Witnesses

The first investigator responding to a report of child abuse or sexual abuse shall refer the child victim for a medical examination. Whenever possible, interviews of child victims and witnesses should be conducted by personnel properly trained in the techniques designed to best elicit truthful information from a child while minimizing additional trauma to the child.

COMMENTARY

Evidence from medical examinations and forensic interviews of children may provide the only corroboration for a successful prosecution of the case, particularly in cases of child abuse. Medical examinations provide documentation of the event and injuries, and forensic interviews gather factual information from a child to determine if the child was the victim of a crime or witnessed a crime against another person. The forensic interview should be appropriate for the child's age and developmental level, but it should not be confused with a therapeutic interview that is conducted for the purpose of designing treatment for and providing treatment to a child.

(3) Address Child Well-Being

Investigators should consider and make inquiry into whether children will be on the scene of an arrest, search warrant, or other enforcement action, and take appropriate actions to address the safety and well-being of children to include involving victim specialists or local child protection agencies as indicated by the circumstances and condition of the children prior to or at the time of the law enforcement action.

COMMENTARY

When assessing a child's well-being, Department personnel should consider whether the child lives in or is exposed to an environment where drugs, including pharmaceuticals, are used, possessed, trafficked, diverted, or manufactured illegally. In such environments, children may experience or be at risk of experiencing physical, sexual, or emotional abuse; medical, educational, emotional, or physical harm; or neglect, including harm resulting or possibly resulting from the inhalation, ingestion, or absorption of illegal drugs. Further, such environments may foster other crimes involving children. For example, children may participate in illegal or sexual activity in exchange for drugs or money likely to be used to purchase drugs.

f. Child Protections During Judicial Proceedings

(1) Child Witnesses

Section 3509 of title 18 provides mechanisms for the protection of child witnesses during judicial proceedings, including closing the courtroom during a child's testimony or allowing the child to testify via alternative means, allowing the use of adult attendants or testimonial aids, and expediting proceedings. Those prosecuting cases involving children should review and are urged to become familiar with the accommodations and protections under applicable law and use them as necessary to protect the interests of child witnesses.

A child is presumed to be competent. The court may permit an attorney, but not a party appearing *pro se*, to examine a child directly on competency, if the court is satisfied that the child will not suffer emotional trauma as a result of the examination. Federal prosecutors should consider making this request of the court because in many instances questioning by a familiar person may be less traumatic for the child. Prosecutors should, however, be aware that defense attorneys likewise may make such a request. (18 U.S.C. § 3509(c)(7)).

(2) Guardian ad Litem

To protect the best interests of the child, the court may appoint a guardian ad litem for a child who was a victim of, or a witness to, a crime involving abuse or exploitation. (18 U.S.C. § 3509(h)(1)). Although 18 U.S.C. § 3509(h) by its terms applies only to cases in which a child is a victim of or witness to abuse or exploitation, prosecutors should consider whether moving for the appointment of a

guardian ad litem would be appropriate in any case in which a child is a victim of or witness to a crime.

(3) Victim Impact Statements

Department personnel should obtain and report to the probation officer accurate information concerning a child's victimization. Children may prepare victim impact statements. Child victim impact statements should be in an age-appropriate format that permits the child to express his or her views concerning the personal consequences of his or her victimization at a level and in a form of communication commensurate with his or her age and ability.

Department personnel should request information from the multidisciplinary child abuse team and other appropriate sources to determine the impact of the offense on the child victim and any other children who may have been affected, in order to provide the probation officer with the most useful and accurate information possible.

2. Victims of Domestic Violence, Sexual Assault, or Stalking

a. Statement of Purpose

Victims' rights laws and policies are of particular importance to victims of domestic violence, sexual assault, or stalking. These crimes often cause emotional trauma in addition to physical injury. It may be more difficult for victims to report these crimes because of the social stigma associated with the crimes and because the victims often have an on-going relationship with the offender. These victims often are in great danger of future violence after reporting a crime, during investigation and prosecution of cases, and after defendants are released from prison. Appropriate responses in these cases can save lives, prevent future violence, and promote victim recovery. Department personnel who work with victims of domestic violence, sexual assault, or stalking should recognize the particular vulnerability of these victims, use their best efforts to respect the privacy and dignity of these victims, and make victim safety a high priority.

b. Specific Guidelines

(1) Evidence of Past Sexual Behavior

Evidence about a victim's past sexual behavior or alleged sexual predisposition is generally inadmissible in court. Prosecutors should be aware of this evidentiary rule and use it when appropriate. (Fed. R. Evid. 412).

(2) Policy Strongly Discouraging Sexual Assault Victim Polygraphs

Department personnel are strongly discouraged from asking sexual assault victims to take polygraph examinations. The investigating agent may ask a sexual

assault victim to take a polygraph examination only in extraordinary circumstances and only with the concurrence of a Special Agent in Charge or the Supervisory Assistant United States Attorney. All reasonable alternative investigative methods should be exhausted before requesting or administering a sexual assault victim polygraph examination.

(3) Referrals for Assistance in Developing a Safety Plan for Domestic Violence Victims

A safety plan is an individualized plan developed by domestic violence victims to reduce the threats of harm they and their family members face. Safety plans include strategies to reduce the risk of physical violence and harm (e.g., obtaining a protective order) and strategies to maintain basic human needs (e.g., housing and income) in spite of the disruptions caused by the victimization, which may include relocation, loss of employment, and physical injury. Victims may need assistance in identifying potential risks to safety and well-being, options for addressing those risks, and information about the types of services and support that may be required from the criminal justice system and community-based providers. Department personnel should consider providing referrals to community-based victim services programs to address those needs. Victim assistance personnel should also be familiar with any programs that exist in the jurisdiction that allow for confidentiality of the victim's address and the requirements for enrollment in those programs.

(4) Limited Testing of Defendants in Sexual Assault Cases

The responsible official shall advise a victim of a sexual assault that poses a "risk of transmission" of the Acquired Immune Deficiency Syndrome (AIDS) virus of the circumstances under which the victim may obtain an order that the defendant be tested for this condition and that the results be shared with the victim. (42 U.S.C. § 14011(b)(1) (2006)).

(5) Payment for Forensic Sexual Assault Examinations

The responsible official or the head of another department or agency that conducts an investigation into a sexual assault shall pay, either directly or by reimbursement to the victim, the cost of a physical examination of the victim and the costs of materials used to obtain evidence. (42 U.S.C. § 10607(c)(7)).

Department personnel should inform the sexual assault victim that he or she may choose to have the department or agency conducting the investigation pay the cost of the examination directly. In no case shall the victim be held responsible for payment for the examination or be required to seek reimbursement for the examination from his or her insurer. Moreover, in no case shall a victim of sexual assault be required to cooperate with law enforcement or prosecution in order to be provided with a forensic medical examination free of charge.

COMMENTARY

Many victims will be reluctant to obtain a forensic sexual assault examination if they know that their insurance company, primary policy holder, and possibly their employer or others will learn of the sexual assault; therefore victims should be informed that they may choose to have the department or agency conducting the sexual assault investigation directly pay the cost of the forensic medical examination.

At the time of an assault, the victim may not be prepared to make a decision to cooperate with the investigation and prosecution of a sexual assault case. Provision of the free forensic exam ensures the evidence is collected and will be available (i) should the victim decide to cooperate, (ii) if the government decides to prosecute without the victim's cooperation, or (iii) if the evidence is needed at a later date.

In cases of sexual assault in Indian Country, it is critically important that the investigative agency fulfill its responsibility to pay for forensic sexual assault examinations because other resources are unlikely to be available, and the absence of a forensic exam may hinder the ability of prosecutors to proceed with a criminal case.

(6) Availability of Payment for Testing and Counseling in Cases of Sexual Assault

The responsible official of the investigative agency shall inform victims of the Attorney General's obligation to pay the costs for up to two anonymous and confidential tests of the victim for sexually transmitted diseases during the 12 months following the assault, and to pay the cost of a counseling session by a medically trained professional regarding the accuracy of such tests and the risk of transmission of sexually transmitted disease to the victim as a result of the assault. (42 U.S.C. § 10607(c)(7)).

(7) Right To Make a Statement About Pretrial Release

The responsible official shall reasonably, and in a timely manner, inform a victim of an interstate domestic violence, violation of a protection order, or stalking offense that he or she has the right to make a statement regarding the danger posed by the defendant for the purpose of determining pretrial release of the defendant or the conditions of such release. (18 U.S.C. § 2263 (2006)).

(8) Mandatory Restitution

The Violence Against Women Act of 1994 (VAWA), Pub. L. No. 103-322, 108 Stat. 1796 (1994), requires courts to order full restitution in cases of sexual abuse (18 U.S.C. § 2248 (2006)) and interstate domestic violence, violation of a protection order, and stalking. (18 U.S.C. § 2264 (2006)).

(9) VAWA Self-Petitioning

VAWA's immigration provisions allow certain battered immigrants to file for immigration relief without their abusers' assistance or knowledge. This relief is available only for the spouses and children of U.S. citizens or aliens lawfully admitted for permanent residence. (8 U.S.C. § 1154 (2006 & Supp. III 2009)); (*see* Article III.H. for additional guidance on immigration relief).

3. Other Vulnerable Victims

a. Accommodation for Unique Vulnerabilities

Department personnel should be aware of the unique challenges that may be present when working with vulnerable victims and witnesses, such as the elderly and persons with physical and mental disabilities. These vulnerable victims and witnesses may have difficulty walking, hearing, or seeing, may be frail, on significant medications, or in chronic pain. Some may have an impaired level of cognitive function, dementia, depression, shame, ambivalence, or fear, which could cause them to be particularly vulnerable and anxious about the criminal justice system. For those vulnerable victims and witnesses who are disabled and homebound, prosecutors may consider the use of depositions, if feasible.

Department personnel should consider helping to make arrangements for transportation to and from court for those victims and witnesses who may not drive, have difficulty walking, or have other physical limitations that make it difficult to attend court proceedings. Arrangements should be made for wheelchairs and assistive listening devices, if needed. To the extent possible, Department personnel should make arrangements with the court in advance to accommodate physical limitations of victims and witnesses, if necessary.

b. Report Suspected Abuse

Whenever Department personnel suspect that an elderly or otherwise vulnerable adult victim or witness may be suffering from neglect, abuse, or exploitation (whether or not the individual is the subject of the matter being investigated or prosecuted), Department personnel should promptly contact the local Adult Protective Services agency or local law enforcement agency to report the concerns. The grounds for reporting such abuse may include physical evidence of abuse, sudden personality changes, disinterest in old habits, and signs of caregiver neglect. In addition, Department personnel should identify and provide referrals to appropriate local social service agencies best able to meet the needs of the victim. Department personnel should also be aware of possible nursing home abuse and report such to the Adult Protective Services or law enforcement agency, or to the state Attorney General's office.

ARTICLE IV

MANDATORY SERVICES

A. Background

The VRRRA mandates Department personnel to provide certain services to “crime victims” starting from the initiation of an investigation. The VRRRA provisions are referred to as “services” to be distinguished from victims’ “rights,” which are contained in the CVRA and are covered in Article V. There is some overlap between rights and services, for example, “reasonable protection” is considered both a right and a service. Each statute, however, has its own definition of crime victim. (*See* Article III for the definitions under each statute). Accordingly, there may be some victims who qualify to receive services who will not be able to enforce crime victims’ rights under the CVRA. This Article primarily addresses the VRRRA victim services provisions.

B. Responsible Officials

The VRRRA requires the Attorney General to designate persons in the Department of Justice who will be responsible for identifying the victims of a crime and performing the services described in that section at each stage of a criminal case. These persons are referred to as “responsible officials” in the statute and the AG Guidelines. (42 U.S.C. § 10607(a)). Responsible officials may delegate their responsibilities under the AG Guidelines to subordinates in appropriate circumstances, but responsible officials remain obligated to ensure that delegated responsibilities are discharged.

The Attorney General designates the following responsible officials:

1. Investigations
 - a. Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF); Drug Enforcement Administration (DEA), and the Federal Bureau of Investigation (FBI) – the Special Agent-in-Charge (SAC) of the division having primary responsibility for conducting the investigation.
 - b. Office of the Inspector General (OIG) – the Inspector General; and
 - c. United States Marshals Service (USMS) – the United States Marshal in whose district the case is being conducted.
2. Once Charges Are Filed

The United States Attorney in whose district the prosecution is pending, unless a Department litigating division is solely litigating the case in which situation the responsible official is the section chief to whom the lead prosecutor reports. By mutual agreement, the United States Attorney and any Department litigating division can transfer

responsible official status to the other entity. Agreements should be in writing and detail how victim obligations are to be fulfilled (*see, e.g., Memorandum from the Acting Assistant Attorney General, Criminal Division, on implementing the Attorney General Guidelines for Victim and Witness Assistance to the Director, Executive Office for United States Attorneys (June 17, 1993)*).

3. Corrections

For cases in which the Bureau of Prisons (BOP) has become involved – the Director or Warden of each BOP facility where the defendant/offender is incarcerated.

4. Parole

For proceedings relating to parole, parole revocation, release to supervision for all parole-eligible offenders, and supervised-release revocation for District of Columbia offenders – the Chairman of the United States Parole Commission.

The responsible official shall designate the personnel who will carry out victim services in each Department of Justice investigating field office, United States Attorney's Office, litigating division, corrections facility, and parole office. The responsible official shall instruct designated personnel to comply with the AG Guidelines and shall delegate to such personnel the authority to carry out the activities thereby required.

C. Timing of Services

Department responsibilities to crime victims begin as soon as possible after the detection of a crime at which they may be undertaken without interfering in the investigation. (42 U.S.C. § 10607(b)). Generally, this point in time is defined by the opening of a criminal investigation. (*See Article III.B.4. for additional guidance on the time parameters for Department obligations.*)

D. Coordination of Services

Department personnel should coordinate with each other in providing victims with the services required by federal law and the AG Guidelines.

The nature and extent of services provided may vary with the type of harm experienced by the victim and other surrounding circumstances. When victims require services provided by personnel from another Department component or other agency, Department personnel should appropriately coordinate with and introduce victims to other components' and agencies' victim assistance personnel. Introductions should include an explanation of each component's role. Department personnel should support each other as members of a team, coordinating services to the greatest possible extent, with a goal of providing consistent services to meet victims' needs.

E. Victim Identification

At the earliest opportunity after the detection of a crime at which it may be done without interfering with an investigation, the responsible official of the investigative agency shall identify the victims of the crime. (42 U.S.C. §10607(b)(1)). Basically, victim identification means identifying the names and contact information for victims. The responsibility for identifying victims continues with the investigative agency throughout the criminal justice process. Other Department components or other investigative agencies may also identify victims, but all identifications should be coordinated with the lead case agent.

For those components having access to the automated Victim Notification System (VNS), identified victims' names and contact information should be entered into VNS as soon as practicable, but no later than at criminal charging. In cases where the identified victim is less than 18 years old, Department personnel should enter the child's date of birth into VNS to facilitate notification when children (who may receive notification through parents or guardians) become adults and are entitled to direct notification. Non-VNS participating components should maintain victims' names and contact information in a format that can be easily converted to the VNS system should the investigation result in a prosecution.

Some specialized types of cases are not entered into VNS during the investigative stage. These include national security investigation/counterterrorism cases. In those cases, responsible officials from the investigative agency should record identified victims' names and contact information in another secure manner.

Identifying and locating victims can be one of the most difficult victim assistance tasks in a case with a large number of victims. Both new technology and traditional law enforcement methods can be utilized to identify victims. For example, officials may use notices on official Web sites or in print or broadcast media to ask victims to contact the agency. Access to a toll-free number can be arranged so that victims can both provide identification information and receive information about available assistance and services. Department employees may also work with hospitals, schools, employers, nonprofit organizations, faith-based organizations, and disaster-assistance centers (where appropriate) to reach out to victims and to secure identification and contact information. In large white-collar crime cases, names and addresses of victims may be obtainable from the defendants' records. For crimes involving aviation disasters, the FBI is the lead investigative agency and has specialized protocols for collecting passenger- and ground-casualty victim information.

F. Reasonable Protection

The investigative agency responsible official shall arrange for a victim to receive reasonable protection from a suspected offender and persons acting in concert with or at the behest of the suspected offender. (42 U.S.C. § 10607(c)(2)). Both the VRRRA and the CVRA use the concept of "reasonable protection." (42 U.S.C. § 10607(c)(2); 18 U.S.C. § 3771(a)(1)). Accordingly, responsible officials shall take reasonable measures to address victims' legitimate

security concerns. Determining the nature and scope of such measures requires an evaluation of the threat level and identification of reasonable options to address that threat within available resources. As with other rights and services, victims may choose to accept or decline any option or options offered by the Department. (*See* Article II.B.). Neither statute requires the Department to provide victims with, for example, bodyguards to ensure their physical security.

The responsibility of arranging for reasonable victim protection remains with the responsible official of the investigative agency throughout the criminal justice process. All Department personnel, however, should consider victims' security concerns at every point in the criminal justice system, and consult and coordinate with the responsible official of the investigative agency concerning victim safety. Any concerns about victim safety and reports of threats should immediately be reported to the lead case agent.

Department personnel should use their discretion and sound judgment when discussing possible threats and security measures with victims. Trained personnel should make victims aware of the resources that may be available to promote their safety. Responsible officials from the investigation, prosecution, and corrections components, as well as the United States Parole Commission, are encouraged to work together to meet the safety concerns of victims. United States Attorneys are encouraged and expected to work with designated responsible officials from investigative components to develop collaborative procedures to meet the safety concerns of victims in their districts.

G. General Information

After the investigative agency opens a case, a responsible official should provide victims with the following general information as needed:

1. **Information About VNS:** Victims should be informed that they will receive notification of case developments through VNS, and may decide at any time to opt out of receiving VNS notifications.
2. **Logistical Information:** Victims should be informed and assisted with respect to transportation, parking, childcare, translator services, and other investigation-related services. Once the prosecution agency files charges, the responsible official of the prosecution agency is responsible for informing and assisting victims with such information in connection with prosecution-related services. Even before the prosecution files charges, the responsible prosecution official should assist victims with logistical information in connection with pre-charging court proceedings such as grand jury appearances. The responsible official of the Parole Commission is responsible for informing and assisting victims with similar services in connection with parole hearings.
3. **Department Employees Who Are Victims of Crime:** The responsible officials of each agency should inform Department employees that they can access an Employee Assistance Program as well as generally available victim assistance programs. Responsible officials should assist employees in accessing appropriate victim services.

4. Information About the Criminal Justice System: During all stages of the process, a responsible official should provide statutory victims with general information about the criminal justice process, specifically including –
 - a. Role: The role of the victim in the criminal justice process, including what the victim can expect from the system as well as what the system expects from the victim.
 - b. Stages: The stages in the criminal justice process that are significant to a crime victim and the manner in which information about such stages can be obtained.

(18 U.S.C. § 1512 note (1984) (Federal Guidelines for Treatment of Crime Victims and Witnesses in the Criminal Justice System); cf. Pub. L. No. 97-291, § 6(a)(1)(C), (D)).
5. Custodial Release Eligibility Information: A responsible official of the custodial agency shall provide the victim with general information regarding the corrections process, including information about work release, furlough, probation, and eligibility for each. (42 U.S.C. § 10607(c)(8)).

H. Services Referrals

At the earliest opportunity after detection of a crime at which it may be done without interfering with an investigation, a responsible official shall provide identified victims with information about services available to them. (42 U.S.C. § 10607(b)(2)). The information shall include the name, title, business address, and telephone number of the responsible official to whom services requests should be addressed (42 U.S.C. § 10607(b)(3)), and the types of services available, including, as appropriate –

1. The place where the victim may receive emergency medical or social services. (42 U.S.C. § 10607(c)(1)(A)).
2. The availability of any restitution or other relief (including crime victim compensation programs) to which the victim may be entitled under this or any other applicable law and the manner in which such relief may be obtained. (42 U.S.C. § 10607(c)(1)(B)).
3. Public and private programs that are available to provide counseling, treatment, and other support to the victim. (42 U.S.C. § 10607(c)(1)(C)).

The responsibility for providing a victim with referrals for services during the investigation lies with the responsible official for the investigative agency. Once an investigation has transferred to the prosecutorial entity or charges are filed, responsible officials from the prosecutorial entity are responsible for ensuring referrals for services are made as appropriate. If a victim has already received referrals for services from the investigative agency, the prosecutorial entity and investigative agency shall employ their best efforts to coordinate any existing and new referrals to ensure consistency, avoid duplication of services, and meet the best interests of the victim and the case.

I. Notice of Case Events

1. During the Investigation

During the investigation of a crime, a responsible official for the investigative agency shall provide the victim with the earliest possible notice concerning –

- a. The status of the investigation of the crime, to the extent that it is appropriate and will not interfere with the investigation. (42 U.S.C. § 10607(c)(3)(A)).
- b. The arrest of a suspected offender. (42 U.S.C. § 10607(c)(3)(B)).

2. During the Prosecution

Responsible officials from the prosecutor's office shall provide notice of court-related case events to victims meeting the VRRRA victim definition. (*See* definition in Article III.B.). The VRRRA requires notice of the following case events:

- a. The filing of charges against a suspected offender. (42 U.S.C. § 10607(c)(3)(C)).
- b. The release or detention status of an offender or suspected offender. (42 U.S.C. § 10607(c)(3)(E)).
- c. The “scheduling of each court proceeding that the witness is either required to attend or . . . is entitled to attend.” (42 U.S.C. § 10607(c)(3)(D)).
- d. The acceptance of a plea of guilty or nolo contendere or the rendering of a verdict after trial. (42 U.S.C. § 10607(c)(3)(F)).
- e. If the offender is convicted, the sentence including the date on which the offender will be eligible for parole, if any. (42 U.S.C. § 10607(c)(3)(G)).

COMMENTARY

Persons meeting the VRRRA victim definition receiving investigative notices should continue to receive prosecution notification either through VNS or other means if VNS is not used. (*See generally* Article V.D.1. regarding VNS coverage). Notices should explain that only victims meeting the CVRA victim definition will be able to assert CVRA rights.

3. During the Corrections Process

a. Custodial Release Notification

After trial, a responsible official from the BOP shall provide a crime victim as defined under the VRRRA (*see* Article III.A.) the earliest possible notice of –

- (1) The escape, work release, furlough, or any other form of release from custody of the offender. (42 U.S.C. § 10607(c)(5)(B)).

- (2) The death of the offender, if the offender dies while in custody. (42 U.S.C. § 10607(c)(5)(C)).

b. Inmate Victims

When the victim is an inmate, the responsible official may take into consideration, in determining when notice is provided, the security of the offender inmate. If there is a serious security risk in informing an inmate victim of an offender's status, the corrections agency may time the notice to minimize that risk, even if the notification takes place after the event. This determination should be made on a case-by-case basis and should not be interpreted to prevent an inmate victim from providing written input in any parole proceeding. The notice requirement in this guideline applies even in cases in which a Department component is holding a defendant (such as a deportable alien) after time served.

c. Prisoner Reentry

In anticipation of an offender's release from custody, the BOP responsible official should take the following actions:

- (1) Victim Impact Statement: If the offender is subject to supervised release in a district other than the district in which the offender was sentenced, the responsible official should transmit the victim impact statement portion of the presentence investigation report to the United States Probation Office in the supervising district.
- (2) Notification Contents: The responsible official should provide a victim with notice of the offender's release date no later than 30 days prior to the offender's release. The notice should also include the city and state in which the offender will be released and, if the offender is subject to supervised release, the supervising United States Probation Office contact information. This notice should also advise the victim to contact the supervising United States Probation Office if the victim receives any threatening communications from the offender. (Note: This renewed notification should not be shared with the offender or his counsel, except as otherwise required by law.)

4. During the Parole Process

After conviction, the responsible official from the Parole Commission shall provide a crime victim as defined under the VRRRA (*see* Article III.B.) with the earliest possible notice of the date on which an offender will be eligible for parole and the scheduling of a parole hearing, if any, for the offender. (42 U.S.C. § 10607(c)(3)(G), (c)(5)(A)).

When an offender violates the conditions of release and a revocation hearing is scheduled, the responsible official from the Parole Commission shall notify the victims of the crime for which parole was granted or supervised release was imposed of the date and time of the revocation proceeding. If the alleged violation is the commission of a new

crime, whether or not the offender has been convicted of the crime, the Parole Commission responsible official should also notify the victims of the new crime.

The Parole Commission responsible official should notify victims in advance of an offender's release to supervision.

5. Victim's Age

Once a child victim reaches 18 years of age, the Department is obligated to provide that victim with notification in cases in which the crime occurred when the victim was a minor. It is also the victim's option to determine who else may receive notification on his or her behalf. Department personnel should take care when initiating the direct notifications, being mindful of the impact on the victim. Department personnel are encouraged to develop specialized procedures to deal with these sensitive situations. In general, Department personnel are encouraged to contact a parent or guardian before the victim's 18th birthday to determine whether the victim is aware of the crime and any special considerations that may be helpful in providing notification. The FBI has developed specialized victim notification procedures for cases involving child pornography. Any Department personnel making notifications in such cases are encouraged to coordinate with the FBI.

J. Separate Waiting Area

During court proceedings, the responsible official shall ensure that a victim is provided with a waiting area removed from and out of the sight and hearing of the defendant and defense witnesses. (42 U.S.C. § 10607(c)(4)).

During parole hearings, the responsible official should coordinate with the United States Marshals Service, BOP, or other entity responsible for the relevant facilities to ensure that a victim is provided with a waiting area that is removed from and out of the sight and hearing of the inmate and the inmate's witnesses. (*See* 42 U.S.C. § 10607(c)(4)).

K. Return of Property

A responsible official from the investigative agency shall ensure that any property of a victim that is being held for evidentiary purposes is maintained in good condition and returned to the victim as soon as it is no longer needed for evidentiary purposes. (42 U.S.C. § 10607(c)(6)). The responsible official from the investigative agency should also, where it does not interfere with the investigation, notify victims that the agency is holding property belonging to the victim. There may be circumstances, however, in which a victim's property will inevitably deteriorate or will be damaged through its utilization in the law enforcement process. Responsible officials may consider advising victims of such circumstances when they arise. Contraband should not be returned to victims.

L. Employer/Debt Notification

Upon request by a victim, the responsible official should assist in notifying –

1. The employer of the victim or witness if cooperation in the investigation/prosecution of the crime causes his or her absence from work.
2. The creditors of the victim or witness, when appropriate, if the crime or cooperation in the investigation/prosecution affects his or her ability to make timely payments.

Upon filing of charges by the prosecutor, this responsibility transfers to the responsible official of the prosecutor's office.

(See 18 U.S.C. § 1512 note (1984) (Federal Guidelines for Treatment of Crime Victims and Witnesses in the Criminal Justice System)).

ARTICLE V

VICTIMS' RIGHTS UNDER THE CVRA

A. Background

The CVRA gives victims in criminal cases eight rights that are enforceable in federal courts. The CVRA “rights” should be distinguished from crime victim “services” contained in VRRRA, which mandates Department personnel to provide certain services to crime victims starting from the initiation of an investigation. (See Article IV.). There is some overlap between the rights and services. For example, “reasonable protection” is considered both a right and a service. Each statute, however, has its own definition of “crime victim.” (See Article III for the definitions under each statute). Accordingly, there may be some victims who qualify to receive services, but who will not have court enforceable rights under the CVRA. This Article primarily addresses the victims’ rights provisions contained in the CVRA.

B. Responsibilities of Department Personnel

1. Best Efforts

Department officers and employees engaged in the detection, investigation, or prosecution of crime shall make their best efforts to see that crime victims (as defined in Article III.C.) are notified of, and accorded, the rights contained in the CVRA (18 U.S.C. § 3771(c)(1)) as early in the criminal justice process as is feasible and appropriate.

2. Advice of Attorney

The prosecutor shall advise the crime victim that the crime victim can seek the advice of an attorney with respect to the CVRA rights. (18 U.S.C. § 3771 (c)(2)). The prosecutor should provide this information as early in the criminal justice process as is feasible and appropriate.

3. Professional Responsibility Considerations

Department attorneys should keep the rules of professional conduct in mind in all interactions with crime victims, including while according crime victims their rights under the CVRA. While the American Bar Association Model Rules of Professional Conduct are referenced below, Department attorneys should consider the specific rules applicable to their conduct, determined by their state(s) of licensure as well as where the case or investigation is proceeding.

Responsible officials should make reasonable efforts to train and properly instruct the non-attorneys who interact with crime victims about attorneys’ obligations under the rules of professional conduct and to ensure non-attorneys’ conduct is compatible with those rules. (See Model Rules of Professional Conduct R. 5.3(b)). In addition, all Department attorneys should keep in mind that they can be held accountable, for professional

responsibility purposes, for the conduct of non-attorneys with whom they work. (See Model Rules of Professional Conduct R. 5.3(c)).

Specifically, Department attorneys should inform crime victims that they do not have an attorney-client relationship with any employee of the Department. Likewise, in dealing with crime victims, Department attorneys should keep in mind their duty of confidentiality to their client, the United States, and not disclose any confidential information of the United States unless the United States consents or the disclosure is impliedly authorized to carry out the representation, including disclosures impliedly authorized as required by the CVRA. (See Model Rules of Professional Conduct R. 1.6).

When dealing with unrepresented victims, Department attorneys should make their role clear, should not state or imply that they are disinterested, and should not give legal advice other than to advise individuals to seek legal counsel. (See Model Rules of Professional Conduct R. 4.3).

A crime victim may seek the legal advice of a non-Department attorney with respect to CVRA rights, and the CVRA provides that the prosecutor shall inform the crime victim that the crime victim may seek the advice of an attorney with respect to the rights contained in the CVRA. (18 U.S.C. § 3771(c)(2)). When a crime victim is represented on the criminal matter, a Department attorney should consider the professional responsibility issues involved in *ex parte* communication with a represented party. Generally, *ex parte* communication with a represented crime victim may be authorized by the CVRA statute to carry out the Department's responsibilities to crime victims as well as authorized by law to carry out investigative activities. (See Model Rules of Professional Conduct R. 4.2).

When Department personnel consider providing victim notification by means that are accessible by the general public, for example, through an unsecure Web site or at an open town hall meeting, personnel should only disclose information that comports with Department and professional responsibility rules limitations. (See Model Rules of Professional Conduct R. 3.6, 3.8(f)). For guidance in particular cases, Department attorneys should consult their Professional Responsibility Officer or the Department's Professional Responsibility Advisory Office.

4. Complaint Process and Sanctions

The Department established the Office of the Victims' Rights Ombudsman (VRO), within the Executive Office for United States Attorneys, to receive and investigate administrative complaints filed by crime victims against its employees, and has implemented procedures in compliance with the CVRA. (Procedures to Promote Compliance With Crime Victims' Rights Obligations, 28 C.F.R. § 45.10(b) (2010)). The complaint process is not designed for the correction of an individual victim's rights violation, but is instead used to request corrective or disciplinary action against Department employees who may have failed to provide crime victims with any of the CVRA rights. A crime victim may file an administrative complaint against employees of the Department. All of

the following offices have identified Victims' Rights Points of Contact, who are responsible for reviewing and investigating victims' complaints, and reporting their results to the VRO for final determination: United States Attorneys' Offices, the Antitrust Division, ATF, BOP, Civil Division's Office of Consumer Litigation, Civil Rights Division, Criminal Division, DEA, Environment and Natural Resources Division, FBI, National Security Division, Tax Division, Parole Commission, and the USMS. The VRO may recommend disciplinary sanctions for Department employees who "wantonly or willfully" fail to provide those rights. (28 C.F.R. § 45.10(e)).

C. Right to Reasonable Protection

A crime victim has the right to be reasonably protected from the accused. (18 U.S.C. § 3771(a)(1)).

Both the CVRA and the VRRRA use the concept of "reasonable protection." (42 U.S.C. § 10607(c)(2); 18 U.S.C. § 3771(a)(1)). Accordingly, responsible officials shall take reasonable measures to address victims' legitimate security concerns. Determining the nature and scope of such measures requires an evaluation of the threat level and identification of reasonable options to address that threat within available resources. As with other rights and services, victims may choose to accept or decline any option or options offered by the Department. (*See* Article II.B.). Neither statute requires the Department to provide victims with, for example, bodyguards to ensure their physical security.

The responsibility of arranging reasonable victim protection remains with the responsible official of the investigative agency throughout the criminal justice process. All Department personnel, however, should consider victims' security concerns at every point in the criminal justice system, and consult and coordinate with the responsible official of the investigative agency concerning victim safety. Any concerns about victim safety and reports of threats should immediately be reported to the lead case agent.

Department personnel should use their discretion and sound judgment when discussing possible threats and security measures with victims. Trained personnel should make victims aware of the resources that may be available to promote their safety.

Responsible officials from the investigation, prosecution, and corrections components, as well as the Parole Commission, are encouraged to work together to meet the safety concerns of victims. U.S. Attorneys are encouraged and expected to work with designated responsible officials from investigative agencies to develop collaborative procedures to meet the safety concerns of victims in their districts.

D. Right to Reasonable, Accurate, and Timely Notice

A crime victim has the right to reasonable, accurate, and timely notice of any public court proceeding, or any parole proceeding, involving the crime or of any release or escape of the accused. (18 U.S.C. § 3771(a)(2); *see also* Fed. R. Crim. P. 60(a)(1)).

1. Automated Victim Notification System (VNS)

For components participating in VNS, victim contact information and notice to victims should be maintained and conducted using VNS. In some circumstances, however, either alternative or additional means of victim notification may be necessary or appropriate. For example, during terrorism investigations VNS is not used, and in some situations, like Indian Country, victims may not have access to postal or computer systems, thereby making VNS impractical.

Responsible officials with access to VNS should enter all necessary information into VNS before transferring notification responsibilities to the next responsible official. In cases where the identified victim is a child, the child's date of birth should be entered into VNS. For specialized guidance on notifying child victims once they become adults, *see* Article IV.I.5. Responsible officials shall use their best efforts to provide all employees with responsibilities related to VNS with adequate training on the proper use of VNS. (*See* Article III.F. for information about notifying victims located in foreign countries).

In the event of an emergency or other last-minute hearing or change in the time or date of a hearing, the responsible official should consider providing notice by telephone or expedited means.

2. Cases With Large Numbers of Victims

a. Individual Notice

According the right to notification in cases with a large number of victims can be challenging. When necessary, Department employees may choose to provide notification solely through electronic means such as via the VNS Web site, e-mail, and call center capabilities.

b. Publication or Proxy Notice

Where the number of victims is so large as to make individual notice to victims impractical, prosecutors should file a motion seeking the court's permission for alternative notification under 18 U.S.C. § 3771(d)(2). Such alternative notification may include publication of notices through media outlets or on public Web sites, or proxy notification to an individual or organization that can disseminate notice to other victims, such as community organizations, corporate entities, or counsel for a class of victims. Multiple forms of outreach may be appropriate in particular cases and creativity is encouraged, with the goal of achieving actual notice to the greatest number of victims possible given the resources available. In every case, Department employees should carefully evaluate the type of information relayed and the method of communication to minimize the risk that investigations are compromised and that victims' privacy interests are inadvertently invaded.

E. Right Not To Be Excluded From Court

A crime victim has the right not to be excluded from any public court proceeding, unless the court, after receiving clear and convincing evidence, determines that testimony by the victim would be materially altered if the victim heard other testimony at that proceeding. (18 U.S.C. § 3771(a)(3); *see also* Fed. R. Crim. P. 60(a)(2)). Before making this determination, “the court shall make every effort to permit the fullest attendance possible by the victim and shall consider reasonable alternatives to the exclusion of the victim from the criminal proceeding.” (18 U.S.C. § 3771(b)(1); *see also* Fed. R. Crim. P. 60(a)(2)). The reason for any decision denying relief shall be clearly stated on the record. (18 U.S.C. § 3771(b)(1); *see also* Fed. R. Crim. P. 60(a)(2)).

1. Victims Who Are Also Witnesses

The crime victim’s right not to be excluded provides statutory authorization for an exception to the *Federal Rules of Evidence*, which mandate that, upon request, the judge exclude witnesses from court so that they cannot hear the testimony of other witnesses. (*See* Fed. R. Evid. 615(4)).

If a victim is a witness, and there is a potential detrimental impact from the victim hearing other witnesses’ testimony, prosecutors should explain any potential detrimental impact so that the victim can make an informed decision whether to exercise this right. If the prosecutor believes that the victim’s testimony would be materially altered if the victim heard other testimony at the proceeding, the prosecutor should inform the victim of this potential divergence of interests and remind the victim that he or she can seek the advice of an attorney in connection with asserting the victim’s rights.

Where appropriate, prosecutors should also make courts aware of the provisions of 18 U.S.C. § 3510, which prohibits a court from ordering a victim excluded from a trial based only on the victim’s exercise of his or her right to be heard during the sentencing hearing for both capital and non-capital cases.

2. Facilitating Attendance

The Department is not required to pay a victim’s expenses to attend court. Department personnel may, however, help victims to identify resources to assist them with the financial burden of court attendance. In addition, Department personnel are not required to transport inmate victims to court for hearings. The travel expenses of victims who are also witnesses, however, should be handled in accordance with Department policy for witness expenses.

3. Non-Public Proceedings

Victims do not have rights to notice of, or to attend or participate in, closed official proceedings. (*See* 18 U.S.C. § 3771(a)(2)-(3)). The government attorney may neither move for nor consent to the closure of a judicial proceeding that is ordinarily open to the public without the express prior authorization of the Deputy Attorney General, based upon

a request processed through the Policy and Statutory Enforcement Unit of the Criminal Division's Office of Enforcement Operations. (*See Policy With Regard to Open Judicial Proceedings*, 28 C.F.R. § 50.9 (2010); USAM 9-5.150). As an example of the type of ordinarily public proceeding falling in this category, closed proceedings will frequently be necessary when a guilty plea is entered by a cooperator whose safety or investigative usefulness might be compromised if information about the plea were made public. Deputy Attorney General approval to close a hearing is not required for traditionally non-public matters, such as grand jury and juvenile proceedings; to prevent psychological harm to a child witness (*see* 18 U.S.C. § 3509(d), (e); 28 C.F.R. § 50.9(e)(5)); and to protect national security information or classified documents. Victims do not have rights to notice of, or attendance or participation at, these closed hearings.

4. Cases With Large Numbers of Victims

In cases with a large number of victims, it may be impractical for each victim to attend personally all the proceedings he or she may wish to attend. In such circumstances, prosecutors should seek the court's permission under 18 U.S.C. § 3771(d)(2) for procedures to accord this right to the greatest extent possible given the resources available. Options include the use of closed circuit television, broadcast of proceedings over a conference call or Web site, or a lottery and schedule for attendance. If the court changes the trial venue, prosecutors should be aware of the provisions of 42 U.S.C. § 10608, which mandates the court to order closed-circuit televising of the proceedings to the original location to permit victims to watch the trial proceedings.

F. Right To Be Reasonably Heard

A crime victim has the right to be reasonably heard at any public proceeding in the district court involving release, plea, sentencing, or any parole proceeding. (18 U.S.C. § 3771(a)(4); *see also* Fed. R. Crim. P. 60(a)(3)).

If a victim (or a lawful representative appearing on behalf of the victim) is present at a covered proceeding and wishes to be heard, the government attorney or prosecutor should advise the court of this fact at an appropriate point in the proceeding. If the prosecutor is aware that a victim or victims will seek to be heard at an upcoming proceeding that involves release, plea, sentencing, or parole, the prosecutor should provide the court with advance notice in accordance with any local rules of procedure or practice.

If the government is seeking the death penalty, and files the proper notice, the responsible official should notify the victim and appropriate family members of their potential opportunity to address the court during the aggravation portion of the sentencing hearing and of the date, time, and place of the scheduled hearing. (*See* 18 U.S.C. § 3593(a) (2006)).

In cases with a large number of victims, it may be impractical for each victim to speak at each opportunity. In such circumstances, prosecutors should seek the court's permission under 18 U.S.C. § 3771(d)(2) for procedures to accord this right to the greatest extent possible given the resources available. Options may include allowing written submissions, limiting

the length of oral presentation, or using a lottery or other method for selecting a limited number of oral statements.

When a defendant is convicted, Department personnel should inform victims that the United States probation officer is required to prepare a presentence investigation report that includes a section assessing the financial, social, psychological, and medical impact of the crime on any individual against whom the offense was committed, including restitution information. (Fed. R. Crim. P. 32(d)(2)(B), (D)). This section is called the Victim Impact Statement (VIS) and Department personnel should inform victims how to communicate directly with the probation officer concerning the VIS if victims choose to do so. Department personnel should also inform the probation officer about any information in the government's possession relevant to the topics addressed in the VIS, particularly concerning the appropriate amount of restitution, if any.

G. Reasonable Right To Confer With the Prosecutor

A crime victim has the reasonable right to confer with the attorney for the government in the case. (18 U.S.C. § 3771(a)(5)).

The victim's right to confer shall not be construed to impair prosecutorial discretion. (*See* 18 U.S.C. § 3771(d)(6)).

1. In General

Federal prosecutors should be available to confer with victims about major case decisions, such as dismissals, release of the accused pending judicial proceedings (when such release is for non-investigative purposes), plea negotiations, and pretrial diversion. (*See* 18 U.S.C. § 1512, Historical and Statutory Notes, Federal Guidelines for Treatment of Crime Victims and Witnesses in the Criminal Justice System). Such conferences should be conducted consistent with applicable rules governing criminal procedure and professional conduct. Ordinarily, prosecutors should use such conferences to obtain relevant information from the victim and convey appropriate nonsensitive or public information to the victim. The conference provides victims the opportunity to express their views, keeping in mind that prosecution decisions are within the prosecutor's discretion. Department personnel should not provide legal advice to victims, either as part of these conferences or otherwise.

2. Proposed Plea Agreements

Prosecutors should make reasonable efforts to notify identified victims of, and consider victims' views about, prospective plea negotiations. Prosecutors should make these reasonable efforts with a goal of providing victims with a meaningful opportunity to offer their views before a plea agreement is formally reached. In circumstances where plea negotiations occur before a case has been brought, Department policy is that this should include reasonable consultation prior to the filing of a charging instrument with the court. Such consultation may be general in nature and does not have to be specific to a particular plea offer or defendant but rather can be a wide solicitation of victim plea

and sentencing views without reference to any particular defendant or person of interest. In determining whether and to what extent consultation is reasonable, the prosecutor should consider factors relevant to the propriety and practicality of giving notice and considering views in the context of the particular case, including, but not limited to, the following factors:

- a. The impact on public safety and risks to personal safety.
- b. The number of victims.
- c. Whether time is of the essence in negotiating or entering a proposed plea.
- d. Whether the proposed plea involves confidential information or conditions or whether some other need for confidentiality is present.
- e. Whether the victim is a possible witness in the case and the effect that relaying any information may have on the defendant's right to a fair trial.

COMMENTARY

The reasonable right to confer concerning possible plea agreements does not obligate the prosecutor to consult with victims every time a term in the plea changes or when particular defendants are added or removed from an investigation or prosecution.

3. Cases With Large Numbers of Victims

In cases where the large number of victims makes individual consultation impractical, Department employees may nonetheless provide victims with information and seek their input through the use of alternative means such as Web sites, e-mails, conference calls, legal representatives, and town hall meetings.

H. Right to Full and Timely Restitution as Provided in Law

Victims have a right to "full and timely restitution as provided in law." (18 U.S.C. § 3771(a) (6)). Restitution is mandatory – regardless of the defendant's ability to pay – for most federal crimes. (*See* 18 U.S.C. § 3663A (2006)). Even when restitution is not mandatory, the sentencing court may require restitution in accordance with a plea agreement (18 U.S.C. § 3663A(a) (3)), or pursuant to the court's discretion. (18 U.S.C. § 3663 (2006 & Supp. II 2008)). In discretionary cases, the court may also require restitution as a condition of probation or supervised release.

All who investigate and prosecute criminal cases play an important role in determining whether restitution is full and timely. The scope of the victim's losses, the nexus between the victim's losses and the crimes charged, what happened to ill-gotten gains, and the defendant's ability to pay are all integral to the criminal prosecution. Restitution should be

considered early in the investigation and throughout the prosecution. Prosecutors have a variety of tools to assure that ill-gotten gains are frozen or forfeited and later restored to victims of crime.

1. Focus on Restitution Early in the Investigation and Throughout the Case

Actions taken at each stage of a case – from investigation, to charging, plea negotiations, and sentencing – all affect whether victims will receive full and timely restitution.

a. Investigation

Investigators should, to the extent reasonably practicable, identify victims and gather information on the extent of victims' losses, the nexus between those losses and the defendant's criminal conduct, and whether any assets exist that might be recovered, frozen, forfeited, or otherwise used to pay restitution.

b. Charging

The amount of restitution that a court may order is affected by the crimes charged. When exercising their discretion, prosecutors should give due consideration to the need to provide full restitution to the victims of federal criminal offenses.

c. Prejudgment Restraint of Assets

Defendants may dissipate or hide their ill-gotten gains as time passes. Prosecutors, during investigations, should consider freezing assets under 18 U.S.C. § 1345 (2006), or seizing assets for criminal or civil forfeiture. In cases where defendants are cooperative, prosecutors may also ask defendants for voluntary, signed agreements not to dissipate assets.

d. Plea Discussions

In plea negotiations, prosecutors should consider "requesting that the defendant provide full restitution to all victims of all charges contained in the indictment or information, without regard to the counts to which the defendant actually plead[s]." (USAM 9-16.320). When reasonably possible, plea agreements should identify victims' losses for purposes of restitution and address the manner of payment. Defendants who can pay some or all of the anticipated restitution should be asked to pay what they reasonably can by the time of sentencing. Under the Sentencing Guidelines, anticipatory payment of restitution is a factor in determining "acceptance of responsibility." (U.S.S.G. § 3E1.1, cmt. n.1(c)).

e. Payments by Sentencing

Defendants who have the ability to pay some or all of their restitution should be asked to pay what they reasonably can by the date of sentencing. (*See generally* 18 U.S.C. § 3572(d)(1) (2006)).

f. Presentence Investigation

Prosecutors and victim witness personnel should help assure that the probation office receives accurate information about victim names, addresses, and amounts subject to restitution. (See 18 U.S.C. § 3664(d)(1) (2006) “[T]he attorney for the government, after consulting, to the extent practicable, with all identified victims, shall promptly provide the probation officer with a listing of the amounts subject to restitution.”). Additionally, if available, information should be provided to the probation office reflecting the defendant’s ability to pay. The presentence report should contain, to the extent reasonably possible, accurate information about the defendant’s financial condition. Prosecutors and their staff should review the presentence report for accuracy as to victim information and the defendant’s ability to pay, and appropriate objections should be raised in a timely fashion.

g. Addressing Issues at Sentencing

Prosecutors and victim witness personnel should help assure that the court has accurate information about victim names, addresses, and loss amounts (inaccurate information may prevent the clerk of the court from disbursing restitution even when funds are available). Federal law provides that “[i]f the victim’s losses are not ascertainable by the date that is 10 days prior to sentencing, the attorney for the Government or the probation officer shall so inform the court, and the court shall set a date for the final determination of the victim’s losses, not to exceed 90 days after sentencing.” (18 U.S.C. § 3664(d)(5)). In rare cases, restitution may not be ordered “if the court finds, from facts on the record, that – (A) the number of identifiable victims is so large as to make restitution impracticable; or (B) determining complex issues of fact related to the cause or amount of the victim’s losses would complicate or prolong the sentencing process to a degree that the need to provide restitution to any victim is outweighed by the burden on the sentencing process.” (18 U.S.C. § 3663A(c)(3)). In such cases, where forfeited assets are involved, prosecutors should consult with the Criminal Division’s Asset Forfeiture and Money Laundering Section (AFMLS) to determine the most effective way of returning forfeited assets to victims. In cases with multiple defendants, the court should be asked to address joint and several liability. (18 U.S.C. § 3664(h)). Additionally, “[i]n any case in which the United States is a victim, the court shall ensure that all other victims receive full restitution before the United States receives any restitution.” (18 U.S.C. § 3664(i)).

h. Orders of Restitution

To assure that restitution issues are addressed fully and accurately, prosecutors should consider tendering an order of restitution in conjunction with the sentencing. The order should identify all victims entitled to restitution, the amount of restitution for each victim, and, where appropriate, prioritization of payments among victims, methods, and schedules for payment, as well as issues of joint and several liability.

i. Payment Plans

By law, if a restitution order “permits other than immediate payment, the length of time over which scheduled payments will be made shall be set by the court, but shall be the shortest time in which full payment can reasonably be made.” (18 U.S.C. § 3572(d)(2)). Payment plans should not be written or construed to prevent enforcement activity post judgment.

COMMENTARY

There are unique restitution issues in tax cases. When the United States seeks restitution in criminal tax cases, prosecutors should take care to avoid compromising the Internal Revenue Service’s ability to collect the civil tax liability. In collecting restitution, prosecutors should be aware that there may be competing claims against the defendant’s assets, including pre-existing tax liens, which may impact the actual amount available for restitution. Prosecutors should consult additional resources and the Tax Division regarding restitution in criminal tax cases and cases where defendants have tax liens.

2. Interplay Between Restitution and Asset Forfeiture

Whenever possible, prosecutors should use asset forfeiture to recover assets to return to victims of crime, as permitted by law. Government attorneys prosecuting civil or criminal forfeiture cases should assist crime victims in obtaining compensation in the following manner. If a defendant has sufficient assets to pay the restitution order without using property forfeitable to the government, the defendant must use those assets (not the forfeitable property) to satisfy the restitution order. If a defendant does not have sufficient assets to pay the restitution order without using forfeitable property, the government may use the procedural provisions of the forfeiture statutes to preserve and recover forfeitable property and to apply such property to the victims of the crime underlying the forfeiture.

There are essentially three methods by which the United States can use assets seized for forfeiture to compensate victims: direct transfers prior to forfeiture; requests for restoration of forfeited funds; and petitions for remission of forfeited funds. The first two methods are intended for use in conjunction with, and to assist in the satisfaction of, a restitution order entered in the criminal case. The third method is available in cases where no restitution order has been entered.

a. Forfeiture Proceedings Termination Before a Final Order of Forfeiture Is Entered

At the request of the United States, the district court may order that funds seized but not finally forfeited to the United States be paid to the clerk of the court toward the satisfaction of the defendant’s restitution obligation. This option is particularly useful when the assets seized are liquid and when the victims are entitled to restitution for

non-pecuniary losses such as physical or emotional injuries, or for other collateral costs that are not compensable under the remission regulations and there are no third-party claimants. (See Provisions Applicable to Victims, 28 C.F.R. § 9.8 (2010)).

b. Request for Restoration

The Restoration Policy set forth in Chapter 13, Section I.B of the *Asset Forfeiture Policy Manual* (2010) and Department of Justice Forfeiture Policy Directive 02-1–Guidelines and Procedures for Restoration of Forfeited Property to Crime Victims via Restitution in Lieu of Remission, allows AFMLS to restore criminally forfeited assets to victims of the offense underlying the forfeiture, who are named in a judicial restitution order, based on the losses recognized in a criminal restitution order. The prosecuting office submits the Request for Restoration on behalf of victims by certifying that the victims named in the court’s restitution order meet the criteria for restoration under the policy. This option is particularly useful when multiple victims have incurred only economic losses, when the interest of third-party claimants must be determined, or when the forfeiture involves property that would be best liquidated by using asset forfeiture procedures.

c. Petition for Remission (Regulations Governing the Remission or Mitigation of Civil and Criminal Forfeitures, 28 C.F.R. pt. 9 (2010)).

Each individual victim can submit a Petition for Remission of judicially forfeited assets to the prosecuting office that obtains a report and recommendation from the seizing agency and then forwards the petition to AFMLS for a final determination. This option is particularly useful when there are victims of offenses that underlie civil forfeitures, but there is no companion criminal case or criminal proceedings terminated prior to conviction, and, thus, no order of restitution. This option is also useful where there is a criminal judgment and order of forfeiture, but the court has declined to issue an order of restitution, for example, where due to the complexity of the proceedings, entry of a restitution order in the criminal case would unduly prolong the underlying criminal proceedings. It is also useful in cases that involve only corporate entities.

3. Enforcement Post Sentencing

After judgments are entered, Financial Litigation Units should prioritize collection activity so that victims may receive full and timely restitution. Financial Litigation Units should investigate defendants’ ability to pay, and should engage in vigorous enforcement methods, which may include filing liens, obtaining writs of execution or garnishment, or adding debtors to the Taxpayer Offset Program.

Victims shall receive timely notice of hearings involving enforcement activities. (18 U.S.C. § 3771(a)(2)).

Prosecutors should be mindful that defendants who knowingly refuse to pay may be resentenced. (18 U.S.C. § 3614(a) (2006)).

I. Right to Proceedings Free From Unreasonable Delay

A crime victim has the right to proceedings free from unreasonable delay. (18 U.S.C. § 3771(a)(7)).

Prosecutors should be reasonably available to consult with victims regarding significant adversities they may suffer as a result of delays in the prosecution of the case and should, at the appropriate time, inform the court of the reasonable concerns that have been conveyed to the prosecutor. Prosecutors should consider raising the victim's right to proceedings free from unreasonable delay when discussing trial dates and responding to defense motions for continuances. Prosecutors should also consider any victim adversities that may result from prosecution requests for continuances and make reasonable efforts to mitigate the delay where possible and consistent with the best interests of the prosecution.

J. Right to Fairness and Respect for Dignity and Privacy

A crime victim has the right to be treated with fairness and with respect for the victim's dignity and privacy. (18 U.S.C. § 3771(a)(8)).

1. Privacy

Consistent with the purposes of 18 U.S.C. § 3771(a)(8), Department personnel engaged in the investigation or prosecution of a crime shall respect victims' privacy and employ best efforts to protect victims' personal information from unnecessary disclosure to the public. (*See* Article II.C.1.).

Press inquiries and other attention from the media often implicate victim privacy concerns. Department personnel should refrain from providing public statements that identify or otherwise allude to the identity of the victim unless warranted for public safety reasons or other appropriate concerns.

2. Dignity

Department personnel should likewise protect the dignity of victims, particularly those victims who have been exploited or are particularly vulnerable (e.g., children, developmentally challenged individuals, mentally ill individuals, or elderly persons). To the extent possible, Department personnel should inform and prepare victims for what evidence or potential testimony will be presented as well as what evidence may be revealed in proceedings. Prosecutors should aim to present material at trial or in hearings in such a manner that balances the presumption of public access to the courts with a victim's right to be treated with dignity. Motions *in limine*, protective orders, and other means should be used to prevent evidence impacting a victim's dignity from unnecessarily being viewed or disclosed in open court or otherwise revealed to the public at large, unless necessary for legitimate evidentiary purposes or to ensure compliance with court rules or rulings.

3. Fairness

Victims have the right to be treated with fairness. While the best interests of the government's case are of primary importance, when responding to motions, arguments, and requests for continuances, Department personnel should consider a victim's right to fairness when developing and presenting the government's position.

Barring legitimate law enforcement considerations, and when feasible under the particular circumstances of the case, Department personnel should use their best efforts to attempt to inform victims about significant public announcements concerning the investigation or prosecution of the case in advance of or concurrent with any Department efforts to inform the public or make a public statement.

K. In-Court Enforcement Mechanisms

Victims' rights under the CVRA may be enforced by motions filed by the government or the victim. (18 U.S.C. § 3771(d)(1); *see also* Fed. R. Crim. P. 60(b)(2)). Department prosecutors are encouraged to assert victims' rights when appropriate, taking into consideration the victim's preferences and the interests of the United States. Prosecutors are urged to analyze any potential issues related to victims' rights early in the case in order to be able to assert victims' rights at the first opportunity. When filing a motion in court, prosecutors should give consideration to victim privacy and take steps to prevent private information from unnecessary disclosure. When a victim files a motion that the Department does not support or that the prosecutor believes is not legally warranted, the government may oppose the motion or refrain from taking a position on the motion. In such circumstances, and whenever prosecutors have questions about enforcement mechanisms, personnel in the United States Attorneys' Offices are encouraged to consult with the Executive Office for United States Attorneys, and those in the litigating divisions are encouraged to consult with their responsible officials.

If the trial court denies a CVRA rights enforcement motion, the movant may petition the Court of Appeals for an expedited writ of mandamus that must issue within 72 hours. (18 U.S.C. § 3771(d)(3)). In addition, on direct appeal, the government may assert as error any denial of victims' rights in the proceeding to which the appeal relates. (18 U.S.C. § 3771(d)(4)). A government attorney seeking to file a petition for a writ of mandamus or a direct appeal must obtain written authorization from the Solicitor General, in addition to the approvals required by that attorney's office or section. *See* 28 C.F.R. § 0.20(b). To facilitate the authorization process, the attorney must prepare a written recommendation as to why appeal or mandamus is warranted in the case, and transmit that recommendation to the attorney's appellate section for them to prepare their own recommendation for the Solicitor General. In cases involving appeals or mandamus requests from divisions other than the Criminal Division, the attorney or the division's appellate section should consult with the Criminal Division's Appellate Section. Because the authorization process will generally

extend beyond the time period for filing a valid notice of appeal, the attorney should file a protective notice of appeal within the applicable time period even though it has not yet been authorized. If the Solicitor General declines to authorize an appeal, the attorney must then file a motion to voluntarily dismiss the appeal.

ARTICLE VI

WITNESSES

A. Victims' Services and Rights Laws Do Not Cover Witnesses

A person who has information or evidence concerning a crime, and provides information regarding his/her knowledge to a law enforcement agency, is a witness. Witnesses who do not fit the CVRA definition of crime victim do not have enforceable victims' rights, and the VRRRA does not require Department personnel to provide witnesses with services. Department personnel should use reasonable efforts to do all that is possible within the limits of available resources, without infringing on the defendant's constitutional rights, to assist witnesses to crime during their interaction with the criminal justice system.

B. Witness Security

Department personnel should take reasonable measures to address the security concerns of witnesses. Determining the nature and scope of such measures requires an evaluation of the threat level and identification of reasonable options to address that threat within available resources. Witnesses have the choice whether to accept the reasonable options the Department offers.

The responsibility of arranging for reasonable witness security remains with the investigative agency throughout the criminal justice process. All Department personnel, however, should consider witness security concerns at every point in the criminal justice system and consult and coordinate with the investigative agency concerning witness security. Witness concerns about safety and reports of threats should immediately be reported to the lead case agent.

Department personnel should use their discretion and sound judgment when discussing possible threats and security measures with witnesses. Trained personnel should make witnesses aware of the resources that maybe available to promote their safety.

Responsible officials from the investigation, prosecution, and corrections components, as well as the Parole Commission, are encouraged to work together to meet safety concerns. United States Attorneys are encouraged to work with responsible officials from investigative agencies to develop collaborative procedures to meet witness safety concerns in their districts.

Admission into the Federal Witness Security Program is an extreme measure that is only available to crucial witnesses in significant prosecutions who are in life-threatening danger. Admission to the Program must be sponsored by a prosecutor and the final determination of Program availability is made by designated officials in the Criminal Division's Office of Enforcement Operations (OEO). Responsible officials in law enforcement agencies and

prosecutor's offices are not authorized to promise witnesses Program admission nor can witnesses rely on such promises absent approval by appropriate OEO officials.

C. Logistical Assistance

Prosecution agencies are responsible for informing and assisting witnesses with information about transportation, parking, childcare, translator services, and other logistical matters in connection with court appearances and witness conferences. The Parole Commission is responsible for informing and assisting witnesses with similar services in connection with parole hearings.

D. Notification of Offender Release

Department personnel may include witnesses in offender release notifications if the situation warrants.

ARTICLE VII

NON-LITIGABILITY

The AG Guidelines are intended to provide internal Department guidance for the treatment of victims of and witnesses to crime, recognizing that the circumstances presented by each case cannot be adequately predicted in advance. Consequently, decisions regarding the treatment of victims of and witnesses to crime frequently will require assessments, evaluations, and the exercise of independent judgment in light of the circumstances presented. The AG Guidelines are not intended to, do not, and should not be relied upon to create any procedural or substantive rights or to establish procedural or substantive standards of conduct or care enforceable at law in any matter, civil or criminal. No limitations are hereby intended or placed on otherwise lawful prerogatives of the Department.

[page intentionally left blank]

APPENDIX A

VICTIMS' RIGHTS AND RESTITUTION ACT (VRRRA), 42 U.S.C. § 10607 (2006)

42 U.S.C § 10607

(a) Designation of responsible officials

The head of each department and agency of the United States engaged in the detection, investigation, or prosecution of crime shall designate by names and office titles the persons who will be responsible for identifying the victims of crime and performing the services described in subsection (c) of this section at each stage of a criminal case.

(b) Identification of victims

At the earliest opportunity after the detection of a crime at which it may be done without interfering with an investigation, a responsible official shall –

- (1) identify the victim or victims of a crime;
- (2) inform the victims of their right to receive, on request, the services described in subsection (c) of this section; and
- (3) inform each victim of the name, title, and business address and telephone number of the responsible official to whom the victim should address a request for each of the services described in subsection (c) of this section.

(c) Description of services

- (1) A responsible official shall –
 - (A) inform a victim of the place where the victim may receive emergency medical and social services;
 - (B) inform a victim of any restitution or other relief to which the victim may be entitled under this or any other law and manner in which such relief may be obtained;
 - (C) inform a victim of public and private programs that are available to provide counseling, treatment, and other support to the victim; and
 - (D) assist a victim in contacting the persons who are responsible for providing the services and relief described in subparagraphs (A), (B), and (C).
- (2) A responsible official shall arrange for a victim to receive reasonable protection from a suspected offender and persons acting in concert with or at the behest of the suspected offender.

- (3) During the investigation and prosecution of a crime, a responsible official shall provide a victim the earliest possible notice of –
 - (A) the status of the investigation of the crime, to the extent it is appropriate to inform the victim and to the extent that it will not interfere with the investigation;
 - (B) the arrest of a suspected offender;
 - (C) the filing of charges against a suspected offender;
 - (D) the scheduling of each court proceeding that the witness is either required to attend or, under section 10606(b)(4) of this title, is entitled to attend;
 - (E) the release or detention status of an offender or suspected offender;
 - (F) the acceptance of a plea of guilty or nolo contendere or the rendering of a verdict after trial; and
 - (G) the sentence imposed on an offender, including the date on which the offender will be eligible for parole.
- (4) During court proceedings, a responsible official shall ensure that a victim is provided a waiting area removed from and out of the sight and hearing of the defendant and defense witnesses.
- (5) After trial, a responsible official shall provide a victim the earliest possible notice of –
 - (A) the scheduling of a parole hearing for the offender;
 - (B) the escape, work release, furlough, or any other form of release from custody of the offender; and
 - (C) the death of the offender, if the offender dies while in custody.
- (6) At all times, a responsible official shall ensure that any property of a victim that is being held for evidentiary purposes be maintained in good condition and returned to the victim as soon as it is no longer needed for evidentiary purposes.
- (7) The Attorney General or the head of another department or agency that conducts an investigation of a sexual assault shall pay, either directly or by reimbursement of payment by the victim, the cost of a physical examination of the victim which an investigating officer determines was necessary or useful for evidentiary purposes. The Attorney General shall provide for the payment of the cost of up to 2 anonymous and confidential tests of the victim for sexually transmitted diseases, including HIV, gonorrhea, herpes, chlamydia, and syphilis, during the 12 months following sexual assaults that pose a risk of transmission, and the cost of a counseling session by a

medically trained professional on the accuracy of such tests and the risk of transmission of sexually transmitted diseases to the victim as the result of the assault. A victim may waive anonymity and confidentiality of any tests paid for under this section.

- (8) A responsible official shall provide the victim with general information regarding the corrections process, including information about work release, furlough, probation, and eligibility for each.

(d) No cause of action or defense

This section does not create a cause of action or defense in favor of any person arising out of the failure of a responsible person to provide information as required by subsection (b) or (c) of this section.

(e) Definitions

For the purposes of this section –

- (1) the term “responsible official” means a person designated pursuant to subsection (a) of this section to perform the functions of a responsible official under that section; and
- (2) the term “victim” means a person that has suffered direct physical, emotional, or pecuniary harm as a result of the commission of a crime, including –
 - (A) in the case of a victim that is an institutional entity, an authorized representative of the entity; and
 - (B) 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):
 - (i) a spouse;
 - (ii) a legal guardian;
 - (iii) a parent;
 - (iv) a child;
 - (v) a sibling;
 - (vi) another family member; or
 - (vii) another person designated by the court.

[page intentionally left blank]

APPENDIX B

CRIME VICTIMS' RIGHTS ACT (CVRA), 18 U.S.C. § 3771 (2006 & SUPP. III 2009)

18 U.S.C. § 3771

(a) Rights of crime victims – A crime victim has the following rights:

- (1) The right to be reasonably protected from the accused.
- (2) The right to reasonable, accurate, and timely notice of any public court proceeding, or any parole proceeding, involving the crime or of any release or escape of the accused.
- (3) The right not to be excluded from any such public court proceeding, unless the court, after receiving clear and convincing evidence, determines that testimony by the victim would be materially altered if the victim heard other testimony at that proceeding.
- (4) The right to be reasonably heard at any public proceeding in the district court involving release, plea, sentencing, or any parole proceeding.
- (5) The reasonable right to confer with the attorney for the Government in the case.
- (6) The right to full and timely restitution as provided in law.
- (7) The right to proceedings free from unreasonable delay.
- (8) The right to be treated with fairness and with respect for the victim's dignity and privacy.

(b) Rights afforded. –

- (1) In general. – In any court proceeding involving an offense against a crime victim, the court shall ensure that the crime victim is afforded the rights described in subsection (a). Before making a determination described in subsection (a)(3), the court shall make every effort to permit the fullest attendance possible by the victim and shall consider reasonable alternatives to the exclusion of the victim from the criminal proceeding. The reasons for any decision denying relief under this chapter shall be clearly stated on the record.
- (2) Habeas corpus proceedings. –
 - (A) In general. – In a Federal habeas corpus proceeding arising out of a State conviction, the court shall ensure that a crime victim is afforded the rights described in paragraphs (3), (4), (7), and (8) of subsection (a).

(B) Enforcement. –

(i) In general. – These rights may be enforced by the crime victim or the crime victim's lawful representative in the manner described in paragraphs (1) and (3) of subsection (d).

(ii) Multiple victims. – In a case involving multiple victims, subsection (d)(2) shall also apply.

(C) Limitation. – This paragraph relates to the duties of a court in relation to the rights of a crime victim in Federal habeas corpus proceedings arising out of a State conviction, and does not give rise to any obligation or requirement applicable to personnel of any agency of the Executive Branch of the Federal Government.

(D) Definition – For purposes of this paragraph, the term “crime victim” means the person against whom the State offense is committed or, if that person is killed or incapacitated, that person's family member or other lawful representative.

(c) Best efforts to accord rights –

(1) Government. – Officers and employees of the Department of Justice and other departments and agencies of the United States engaged in the detection, investigation, or prosecution of crime shall make their best efforts to see that crime victims are notified of, and accorded, the rights described in subsection (a).

(2) Advice of attorney. – The prosecutor shall advise the crime victim that the crime victim can seek the advice of an attorney with respect to the rights described in subsection (a).

(3) Notice. – Notice of release otherwise required pursuant to this chapter shall not be given if such notice may endanger the safety of any person.

(d) Enforcement and limitations. –

(1) Rights. – The crime victim or the crime victim's lawful representative, and the attorney for the Government may assert the rights described in subsection (a). A person accused of the crime may not obtain any form of relief under this chapter.

(2) Multiple crime victims. – In a case where the court finds that the number of crime victims makes it impracticable to accord all of the crime victims the rights described in subsection (a), the court shall fashion a reasonable procedure to give effect to this chapter that does not unduly complicate or prolong the proceedings.

(3) Motion for relief and writ of mandamus. – The rights described in subsection (a) shall be asserted in the district court in which a defendant is being prosecuted for the crime or, if no prosecution is underway, in the district court in the district in

which the crime occurred. The district court shall take up and decide any motion asserting a victim's right forthwith. If the district court denies the relief sought, the movant may petition the court of appeals for a writ of mandamus. The court of appeals may issue the writ on the order of a single judge pursuant to circuit rule or the Federal Rules of Appellate Procedure. The court of appeals shall take up and decide such application forthwith within 72 hours after the petition has been filed. In no event shall proceedings be stayed or subject to a continuance of more than five days for purposes of enforcing this chapter. If the court of appeals denies the relief sought, the reasons for the denial shall be clearly stated on the record in a written opinion.

- (4) Error. – In any appeal in a criminal case, the Government may assert as error the district court's denial of any crime victim's right in the proceeding to which the appeal relates.
- (5) Limitation on relief. – In no case shall a failure to afford a right under this chapter provide grounds for a new trial. A victim may make a motion to re-open a plea or sentence only if –
 - (A) the victim has asserted the right to be heard before or during the proceeding at issue and such right was denied;
 - (B) the victim petitions the court of appeals for a writ of mandamus within 14 days; and
 - (C) in the case of a plea, the accused has not pled to the highest offense charged.

This paragraph does not affect the victim's right to restitution as provided in title 18, United States Code.

- (6) No cause of action. – Nothing in this chapter shall be construed to authorize a cause of action for damages or to create, to enlarge, or to imply any duty or obligation to any victim or other person for the breach of which the United States or any of its officers or employees could be held liable in damages. Nothing in this chapter shall be construed to impair the prosecutorial discretion of the Attorney General or any officer under his direction.
- (e) Definitions. – For the purposes of this chapter, the term "crime victim" means a person directly and proximately harmed as a result of the commission of a Federal offense or an offense in the District of Columbia. In the case of a crime victim who is under 18 years of age, incompetent, incapacitated, or deceased, the legal guardians of the crime victim or the representatives of the crime victim's estate, family members, or any other persons appointed as suitable by the court, may assume the crime victim's rights under this chapter, but in no event shall the defendant be named as such guardian or representative.

(f) Procedures to promote compliance. –

- (1) Regulations. – Not later than 1 year after the date of enactment of this chapter, the Attorney General of the United States shall promulgate regulations to enforce the rights of crime victims and to ensure compliance by responsible officials with the obligations described in law respecting crime victims.
- (2) Contents. – The regulations promulgated under paragraph (1) shall –
 - (A) designate an administrative authority within the Department of Justice to receive and investigate complaints relating to the provision or violation of the rights of a crime victim;
 - (B) require a course of training for employees and offices of the Department of Justice that fail to comply with provisions of Federal law pertaining to the treatment of crime victims, and otherwise assist such employees and offices in responding more effectively to the needs of crime victims;
 - (C) contain disciplinary sanctions, including suspension or termination from employment, for employees of the Department of Justice who willfully or wantonly fail to comply with provisions of Federal law pertaining to the treatment of crime victims; and
 - (D) provide that the Attorney General, or the designee of the Attorney General, shall be the final arbiter of the complaint, and that there shall be no judicial review of the final decision of the Attorney General by a complainant.



Attorney General Guidelines for Victim and Witness Assistance

For copies of this report and/or additional information,
please contact

OVC Resource Center
P.O. Box 6000
Rockville, MD 20849-6000
Telephone: 1-800-851-3420 or 301-519-5500
(TTY 1-877-712-9279)
www.ncjrs.gov

Or order OVC publications online at www.ncjrs.gov/App/Publications/AlphaList.aspx.
Submit your questions to Ask OVC at <http://ovc.ncjrs.gov/askovc>.
Send your feedback on this service via www.ncjrs.gov/App/Feedback.aspx.

Refer to publication number NCJ 235121.

For information on training and technical
assistance available from OVC, please contact

OVC Training and Technical Assistance Center
9300 Lee Highway
Fairfax, VA 22031
Telephone: 1-866-OVC-TTAC (1-866-682-8822)
(TTY 1-866-682-8880)
www.ovcttac.gov

U.S. Department of Justice
Office of Justice Programs
Office for Victims of Crime

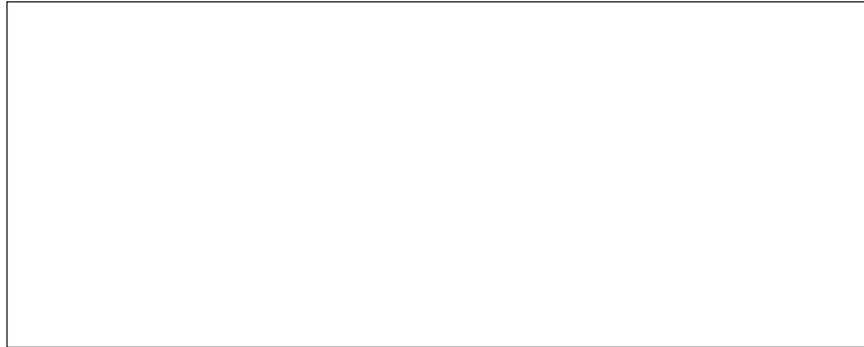
Washington, DC 20531

Official Business

Penalty for Private Use \$300



MEDIA MAIL POSTAGE & FEES PAID DOJ/OVC PERMIT NO. G-91



ATTACHMENT B

INITIAL INFORMATION FOR VICTIMS AND WITNESSES OF CRIME
(DD FORM 2701)

increased concern for their personal safety and that of their family, trouble concentrating on the job, difficulty handling everyday problems, feeling overwhelmed, and thinking of the crime repeatedly.

Some or all of these behaviors may occur and will ease with time. They are normal reactions but you may wish to see a counselor. State compensation funds may be available to reimburse you for such counseling. The Victim/Witness Assistance Responsible Official will have further information.

Your Rights As A Victim.

As a Federal crime victim, you have the following rights:

- The right to be treated with fairness and with respect for your dignity and privacy;
- The right to be reasonably protected from the accused offender;
- 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 your testimony would be materially affected if you as the victim heard other testimony at trial;
- The right to confer with the attorney for the government in the case;
- The right to available restitution;
- The right to information about the conviction, sentencing, imprisonment, and release of the offender.

If You Need Additional Assistance:

In regard to the status of the investigation, contact the investigator below:

(Name)

(Telephone Number)

In regard to other assistance available, contact the command Victim/Witness Responsible Official, or the person identified below:

(Name)

(Telephone Number)

In regard to the prosecution, contact the legal office below:

(Name)

(Telephone Number)

In regard to compensation for medical or other expenses, contact the state office for Crime Victim Compensation:

(Name)

(Telephone Number)

Please notify these offices of any changes of address or telephone number.

For further information on crime issues, see the DoD Victim and Witness Assistance Council web page at:
<http://dod.mil/vwac>

Reset

DEPARTMENT OF DEFENSE



INITIAL INFORMATION FOR VICTIMS AND WITNESSES OF CRIME

DD FORM 2701, MAY 2004

Previous edition is obsolete.
Adobe Professional 7.0

Initial Information
For Victims and Witnesses of Crime

Introduction. We are concerned about the problems often experienced by victims and witnesses of crime. We know that as a victim or witness, you may experience anger, frustration, or fear as a result of your experience. The officer responsible for Victim/Witness Assistance at your installation can help.

We have prepared this brochure to help you deal with the problems and questions which often surface during an investigation and to provide you with a better understanding of how the military criminal justice system works. Your continued assistance is greatly needed and appreciated.

A criminal investigation can be both complex and lengthy and may involve several agencies, some Federal and some local. If you request, you will be kept informed of the status of your case by the investigator handling your case. His or her name is on the back of this brochure.

If You Are Threatened Or Harassed.

If anyone threatens you or you feel that you are being harassed because of your cooperation with this investigation, contact the investigator or the Victim/Witness Responsible Official right away. It is a crime to threaten or harass a victim or witness.

If You Were Injured. If you do not have insurance to pay the cost of your medical or counseling bills, or related expenses, the state Crime Victim Compensation office may be able to assist.

If You Were a Victim of Spouse or Child Abuse.

For your safety, you may want a restraining order, or temporary shelter. For information about these steps or about counseling services, call the Victim/Witness Responsible Official. If the offender is convicted or discharged for abusing you or your children, you may be eligible for "transitional compensation" benefits. Contact the prosecutor identified on the back of this brochure for further information.

Restitution. If an individual is arrested and prosecuted in federal court, you may be eligible for restitution. Restitution is court-ordered payment to you as a victim of crime. It is made by the offender for any out of pocket expenses caused by the crime. Restitution cannot be ordered as a sentence in a military court-martial, but it can be used as a condition of a pre-trial agreement to plead guilty to an offense, or as a condition of clemency or parole.

If Property Was Stolen. If your property was stolen, we hope to recover it as part of our investigation. If we do, we will notify you and return it to you as quickly as possible. Sometimes property needs to be held as evidence for trial. We will return your property once it is no longer needed as evidence.

If You Need Assistance With Your Employer or Command. If you have problems at work because of the crime or the investigation, we can contact your employer or Commanding Officer to discuss the importance of your role in the case.

If An Arrest Is Made. If you ask, you will be notified if a suspect is arrested. Since criminal defendants may be released before trial, you can ask for a restraining order to help protect you from the suspect.

Trial. Once an offense has been referred to trial, you will be contacted by the military trial counsel (prosecutor) or the Assistant U.S. Attorney assigned to handle your case, as appropriate. Each command and U.S. Attorney has a Victim/Witness Responsible Official to help answer your questions and deal with your concerns during the prosecution. You have the right to be consulted at key stages in the trial and will be informed of these rights by trial counsel.

Confinement. If the accused is sentenced to confinement (prison), you have a right to notification of changes in the confinee's status. Use a DD Form 2704, "Victim/Witness Certification and Election Concerning Inmate Status", to request that the confinement facility notify you of parole hearings, escape, release, or death of the confinee.

The Emotional Impact of Crime. Many victims and witnesses are emotionally affected by the crime. Although everyone reacts differently, victims and witnesses report some common behaviors, such as

ATTACHMENT C

**SAMPLE DD FORM 2701, INITIAL INFORMATION FOR VICTIMS AND
WITNESSES OF CRIME**

increased concern for their personal safety and that of their family, trouble concentrating on the job, difficulty handling everyday problems, feeling overwhelmed, and thinking of the crime repeatedly.

Some or all of these behaviors may occur and will ease with time. They are normal reactions but you may wish to see a counselor. State compensation funds may be available to reimburse you for such counseling. The Victim/Witness Assistance Responsible Official will have further information.

Your Rights As A Victim.

As a Federal crime victim, you have the following rights:

- The right to be treated with fairness and with respect for your dignity and privacy;
- The right to be reasonably protected from the accused offender;
- 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 your testimony would be materially affected if you as the victim heard other testimony at trial;
- The right to confer with the attorney for the government in the case;
- The right to available restitution;
- The right to information about the conviction, sentencing, imprisonment, and release of the offender.

If You Need Additional Assistance:

In regard to the status of the investigation, contact the investigator below:

Jane Smith

(Name)
(999)123-4567

(Telephone Number)

In regard to other assistance available, contact the command Victim/Witness Responsible Official, or the person identified below:

Tom Jones

(Name)
(555)123-4567

(Telephone Number)

In regard to the prosecution, contact the legal office below:

AUSA Susan Johnson

(Name)
(999)456-7890

(Telephone Number)

In regard to compensation for medical or other expenses, contact the state office for Crime Victim Compensation:

Ryan Help

(Name)
(999)789-1234

(Telephone Number)

Please notify these offices of any changes of address or telephone number.

For further information on crime issues, see the DoD Victim and Witness Assistance Council web page at:
<http://dod.mil/vvwac>

DEPARTMENT OF DEFENSE



INITIAL INFORMATION FOR VICTIMS AND WITNESSES OF CRIME

Reset

DD FORM 2701, MAY 2004

Previous edition is obsolete.
Adobe Professional 7.0

ATTACHMENT D

ANNUAL REPORT ON VICTIM AND WITNESS ASSISTANCE (DD FORM 2706)

ANNUAL REPORT ON VICTIM AND WITNESS ASSISTANCE				REPORT CONTROL SYMBOL DD-P&R(A)1952	
This report summarizes delivery of services to victims and witnesses as prescribed by the Victim and Witness Protection Act of 1982 (18 USC 1512) and the Victim's Rights and Restitution Act of 1990 (42 USC 10601-10607). It is submitted annually in accordance with DoD Instruction 1030.2.					
1. REPORTING OFFICE			2. REPORTING PERIOD		
			a. FROM		b. TO
			January 1,		December 31,
3. DURING THE REPORTING PERIOD, OUR LAW ENFORCEMENT, SPECIAL INVESTIGATION, TRIAL COUNSEL, AND RELATED OFFICES ASSISTED:					
a. UPON INITIAL CONTACT: _____ crime victims and _____ witnesses were informed of their rights to assistance (DD Form 2701).					
b. UPON REFERRAL TO COURT-MARTIAL: _____ crime victims were informed of their consultation rights in courts-martial (DD Form 2702).					
c. UPON SENTENCING TO CONFINEMENT: _____ crime victims and _____ witnesses were informed of their right to be notified of changes in the confinee's status in prison (i.e., escape, parole, death) (DD Form 2703).					
d. ONCE INFORMED OF THEIR RIGHT TO BE NOTIFIED OF CHANGES IN THE CONFINEE'S STATUS: _____ crime victims and _____ witnesses, using the DD Form 2704, elected to be notified of confinee status changes.					
4. DURING THE REPORTING PERIOD: _____ confinee status changes resulted in _____ notification letters (DD Form 2705) being sent from our confinement facilities.					
5. AS OF DECEMBER 31, _____ Our confinement facilities reported the <u>cumulative</u> total of Service confinees for whom they must make victim or witness notifications as follows:					
(1) ARMY	(2) NAVY	(3) AIR FORCE	(4) MARINES	(5) COAST GUARD	(6) OTHER
6. DOD COMPONENT RESPONSIBLE OFFICIAL					
a. NAME (Last, First, Middle Initial)		b. SIGNATURE		c. DATE SIGNED (YYYYMMDD)	

CHAPTER 24

PROTECTIVE SERVICE PROGRAM

<u>Contents</u>	<u>Section</u>
Purpose	24.1
Definitions	24.2
Foundational Authorities	24.3
Designation of Principals	24.4
Responsibilities	24.5
PSO Team Selection	24.6
Training	24.7
Documentation of PSO Activities	24.8
Assistance to Partner PPOs	24.9
Overtime Pay	24.10
Equipment Procurement and Maintenance	24.11

24.1. **Purpose.** This chapter implements authority for the Defense Criminal Investigative Service (DCIS) to conduct Protective Service Operations (PSO). Specific guidance for the operational planning, conduct, or training for PSOs can be found in the DCIS PSO Handbook. A link to the PSO Handbook can be found in the DCIS Toolbox.

24.2. **Definitions**

24.2.a. **Family Member.** Individuals defined as “dependent” in section 1072(2), title 10, United States Code (U.S.C.), include spouses, unmarried widows, unmarried widowers, and unmarried legitimate children, including adopted children or stepchildren, who are under 21, incapable of self-support, or under 23 and enrolled in a full-time education institution.

24.2.b. **High Risk Billet (HRB).** Authorized personnel billet (identified and recommended by the appropriate authority) that because of grade (normally O-8 or ES-03/04 or higher), assignment, travel itinerary, or symbolic value may make a person filling it an especially attractive or accessible target.

24.2.c. **High Risk Personnel (HRP).** Personnel who, by their grade, assignment, symbolic value, or relative isolation are likely to be an attractive or accessible target.

24.2.d. **HRP Level 1 Protection.** Protective security detail support provided to an official who requires continuous protection as recommended by a Personal Security Vulnerability Assessment (PSVA) and authorized by the Deputy Secretary of Defense (DEPSECDEF).

24.2.e. **HRP Level 2 Protection.** Protective security detail support to an official who requires protection during periods of official duty or travel as recommended by a PSVA and authorized by the DEPSECDEF.

24.2.f. **HRP Level 3 Protection.** Support provided to an official who requires advanced individual antiterrorism awareness and personal protection training.

24.2.g. **Personal Security Vulnerability Assessment (PSVA).** An assessment to determine the vulnerability of a particular individual to an attack. Identifies specific areas of improvement to withstand, mitigate, or deter acts of violence or terrorism against the individual.

24.2.h. **Principal.** An individual requiring the protection of a PSO. A principal may be an HRP or a distinguished visitor.

24.2.i. **Protection-Providing Organization (PPO).** As defined in DoDI O-2000.22, refers collectively to the Army Criminal Investigation Command (Army CID), the Naval Criminal Investigative Service (NCIS), the Air Force Office of Special Investigations (AFOSI), the DCIS, Pentagon Force Protection Agency (PFPA), and the National Security Agency (NSA).

24.2.j. **Protective Service.** A specialized activity that increases the personal safety and security of a principal or other distinguished visitor. The protection activity may be limited in scope or may involve considerable amount of staffing and resources.

24.2.k. **Protective Security Team (PST).** A trained security team used to protect an HRP from assassination, kidnapping, injury, and embarrassment.

24.2.l. **Protective Service Operation (PSO).** The use of specialized procedures and operational techniques by trained personnel to ensure a principal's personal safety and security during a specific event, while traveling, or over an extended period of time. When required, a PSO can be tailored to provide 24-hour protection.

24.2.m. **Protective Threat Assessment (PTA).** Collection and analysis of information to 1) identify the potential for and threats to harm, seize, interfere with, or embarrass a specific principal, and 2) determine the existing and anticipated security environment.

24.2.n. **Security Advisor.** A DCIS special agent assigned overall responsibility for the personal safety and security of a principal. The security advisor is authorized to make decisions on all matters concerning the immediate personal safety and security of the principal. The security advisor is also the PSO Team Leader when a PSO is active.

24.3. **Foundational Authorities**

24.3.a. Under Public Law 110-181, section 1074, "The Secretary of Defense, under regulations prescribed by the Secretary and in accordance with the guidelines approved by the Secretary and the Attorney General, may authorize qualified members of the Armed Forces and qualified civilian employees of the Department of Defense to provide physical protection and personal security within the United States..."

24.3.b. DoD Instruction (DoDI) O-2000.22, "Designation and Physical Protection of DoD High Risk Personnel (HRP)," specifically identifies DCIS as one of six DoD PPOs.

24.3.c. Section 1585a, title 10, U.S.C., specifically confers upon DCIS agents the authority to execute warrants and make arrests, including warrantless arrests, under Attorney General Guidelines.

24.3.d. Section 1114, title 18, U.S.C., makes it a felony for anyone who “kills or attempts to kill any officer or employee of the United States...”

24.3.e. Use of Force guidelines applicable to DCIS agents conducting PSOs are contained in Special Agents Manual (SAM) Chapter 38, “Use of Force.”

24.4. Designation of Principal

24.4.a. Public Law 110-181 authorizes the Secretary of Defense to provide physical protection and personal security to:

24.4.a.(1). any official, military member, or employee of the DoD;

24.4.a.(2). a former or retired official who faces serious and credible threats;

24.4.a.(3). members of the immediate family of a person authorized to receive physical protection and personal security under certain circumstances;

24.4.a.(4). a head of a foreign state, an official representative of a foreign government, or any other distinguished foreign visitor to the United States who is primarily conducting official business with the Department of Defense; and

24.4.a.(5). an individual who has been designated by the President, and who has received the advice and consent of the Senate, to serve as Secretary of Defense, but who has not yet been appointed.

24.4.b. DoDI O-2000.22 designates select positions as HRBs which require a permanent level of protection provided to individuals filling these billets. Officials serving in these billets are considered HRP. Permanent HRBs are identified in DoDI O-2000.22. Individuals may be nominated for HRP status based upon a credible threat documented in a current PSVA. The DEPSECDEF authorizes all HRP nominations.

24.4.c. In the event of a credible threat against the DoD Inspector General or a DoD OIG employee necessitating an HRP nomination, the Protective Services Program Manager (PSPM) will draft and submit an HRP nomination package to the DEPSECDEF.

24.4.d. DoDI O-2000.22 does not apply to physical protection of personnel in combat zones. HRBs in contingency areas are handled in accordance with DoDI 2000.16, DoD Antiterrorism (AT) Standards.

24.5. **Responsibilities**

24.5.a. **Deputy Inspector General for Investigations (DIG-INV).** The DIG-INV has the overall responsibility for the DCIS PSO Program. The DIG-INV designated the Assistant Inspector General for Investigations, International Operations (AIGI-International) as the authority for program oversight and management. The DIG-INV maintains authority to direct the missions and conduct of the PSO Team, including the assignment of tasks to the PSO that may not be expressly cited in DoDI O-2000.22, including the temporary assignment of the PSO Team to evaluate threats against DoD OIG personnel and DoD OIG interests.

24.5.b. **Director, National Security Programs (05NS).** The Program Director (05NS) has primary responsibility for the overall programmatic focus and function of the DCIS PSO program.

24.5.c. **Protective Services Program Manager (PSPM).** The PSPM is the office of primary responsibility for the daily oversight and administration of the DCIS PSO program and the PSO Team. The DCIS PSPM will perform the following functions.

24.5.c.(1). Disseminate all DCIS PSO policy and procedural guidance.

24.5.c.(2). Identify PSO Team training requirements to the DCIS Investigative Operations Directorate/Training to ensure sufficient numbers of properly trained personnel to accomplish the PSO mission.

24.5.c.(3). Identify and budget for procurement of specialized protective services equipment. On an annual basis, the PSPM will identify unmet budgetary, personnel, equipment or other resource requirements and the impact of those unmet requirements on DCIS' ability to perform protective services. Any shortfalls for budgetary reasons will be documented and addressed to the extent possible by the PSPM and kept on file to track the readiness of the PSO team/personnel.

24.5.c.(4). Through coordination with Field Office leadership, ensure DCIS PSO members are available to assist the other DoD PPOs for joint PSOs and other protective assistance if called upon.

24.5.c.(5). Initiate, review, and approve all vulnerability assessments, threat assessments, and threat protection plans produced by DCIS in support of HRPs, potential HRPs, and other mission requirements.

24.5.c.(6). Coordinate outside requests for PSO operational support, e.g., manpower, equipment, etc., that require DCIS resources.

24.5.d.(7). Document the activities of the DCIS PSO Team in accordance with section 24.8 below.

24.6. PSO Team Selection

24.6.a. The DCIS PSO Team shall consist of the PSPM, six to eight team members in the National Capitol Region, and at least one team member each from the Northeast Field Office, Southeast Field Office, Central Field Office, Southwest Field Office, and Western Field Office.

24.6.b. To the extent possible, the DCIS PSO Team will consist of volunteers solicited by 05NS and approved by the cognizant Special Agent in Charge.

24.7. Training

24.7.a. In accordance with DoDI O-2000.22, all personnel participating in the DCIS Protective Service Program are required to attend the Federal Law Enforcement Training Center (FLETC) Protective Service Operations Training Program (PSOTP), the NCIS PSO Training Program, or equivalent protective services training. Equivalent training will be approved by the Program Director, National Security.

24.7.b. In addition, PSO Team members will perform at least 5 days annual operational PSO duties (CONUS and OCONUS) and at least 5 days annual DCIS team training. The PSPM is responsible for scheduling all joint operational PSO assignments and PSO Team training. These requirements may be waived for individual agents on a case by case basis. Requests for waiver of either the annual operational PSO duties requirement or the annual DCIS team training requirement will be submitted through the PSPM to the Director, National Security Division. No more than one waiver will be granted during any three year period.

24.7.c. At least two members of the PSO Team will be trained to conduct PSVAs. PSVA-qualified PSO Team members must attend the FLETC Physical Security Training Program or equivalent training approved by the Program Director, National Security.

24.8. Documentation of PSO Activities

24.8.a. PSVAs, DCIS-led PSOs, DCIS training, and joint PSO missions associated with the Protective Service Program will be documented by the PSPM in the Case Reporting and Information Management System (CRIMS). The PSPM will initiate an annual PSO project to track PSO activities and agent hours. The initiation and closing of the PSO Project will coincide with the annual performance period. Reporting will conform to the requirements set forth in SAM Chapter 28, "Investigative Reports."

24.9. Assistance to Partner PPOs

24.9.a. To the extent possible, DCIS shall provide mutual assistance to PFPA, NCIS, Army CID, AFOSI, and NSA upon request. Joint PSO missions provide opportunities for DCIS PSO Team members to gain experience during actual operations and contribute to efficiency across the DoD PSO mission by reducing the requirement for all PPOs to maintain large standing details.

24.9.b. PSO Team members may only participate in joint PSO missions scheduled by DCIS with the concurrence of the AIGI-International.

24.9.c. DCIS may be tasked by the Director, Security Support for the Secretary of Defense (SECDEF), to provide support for the protection of the SECDEF and DEPSECDEF.

24.10. **Overtime Pay**

24.10.a. **Authority.** IG Instruction 1422.1, “Tours of Duty, Overtime, Time and Attendance Reporting,” May 2, 2011, and SAM Chapter 54, “Law Enforcement Availability Pay,” contain authority and guidance regarding overtime pay for GS-1811 criminal investigators receiving Law Enforcement Availability Pay (LEAP). DCIS PSO Team members shall be paid overtime pay in accordance with current policy.

24.10.b. **Procedure.** Unless otherwise directed by SAM Chapter 54, the PSPM shall utilize Air Force Form 428, “Request for Overtime, Holiday Premium Pay, and Compensatory Time,” to obtain authorization for overtime pay for PSO Team members. Requests will be forwarded to the Deputy Assistant Inspector General for Investigations, International Operations, or designee for approval prior to the beginning of the pay period covered by the request.

24.10.c. **Requests for Overtime Pay.** PSPM will incorporate and evaluate the following information when requesting overtime pay.

24.10.c.(1). The work to be performed during overtime hours.

24.10.c.(2). Why such work could not be performed during regular work hours.

24.10.c.(3). An estimate of the total number of overtime hours required.

24.10.c.(4). The dates which the overtime is to be performed.

24.10.c.(5). Coordinate if DCIS PSO Team Members request compensatory time off in lieu of overtime pay.

24.11. **Equipment Procurement and Maintenance**

24.11.a. All equipment requirements and required funding requests are the responsibility of the PSPM.

CHAPTER 25

COORDINATION OF REMEDIES

<u>Contents</u>	<u>Section</u>
References	25.1.
General	25.2.
Security Clearance Suspensions and Revocations	25.3
Definitions	25.4.
Suspension	25.5.
Debarment	25.6.
Reporting Requirements	25.7.
SDO Duties	25.8.

25.1. References

25.1.a. DoD Instruction 7050.05, “Coordination of Remedies for Fraud and Corruption Related to Procurement Activities,” May 12, 2014.

25.1.b. DOJ, U.S. Attorney’s Manual (USAM) Title 1-12.000; Coordination of Parallel Criminal, Civil, Regulatory, and Administrative Proceedings, February 2013.

25.1.c. Federal Acquisition Regulation (FAR), Subpart 9.4, “Debarment, Suspension, and Ineligibility.”

25.1.d. DoD FAR Supplement (DFARS), Subpart 209.4, “Debarment, Suspension, and Ineligibility.”

25.1.e. Executive Order 12549, Debarment and Suspension, February 18, 1986.

25.1.f. Title 32, Code of Federal Regulations, Part 25, “Government-wide Debarment and Suspension (Nonprocurement).”

25.1.g. Title 10, United States Code, Section 2393, “Prohibition Against Doing Business with Certain Offerors or Contractors.”

25.1.h. DoD Instruction 4140.01, “DoD Supply Chain Materiel Management Policy,” December 14, 2011.

25.1.i. DoD Instruction 4140.67, “Counterfeit Prevention Policy,” April 26, 2013.

25.1.j. DoD Directive 5105.42, “Defense Security Service,” August 3, 2010, (Incorporating Change 1, March 31, 2011).

25.1.k. DoD Instruction 5200.2-R, “DoD Personnel Security Program,” March 21, 2014, (Incorporating Change 1, Effective September 9, 2014)

25.2. General

25.2.a. This chapter contains policies and procedures regarding the coordination of administrative remedies that may be taken in response to evidence or credible information of misconduct stemming from investigations conducted by the Defense Criminal Investigative Service (DCIS).

25.2.b. DoD Instruction 7050.05 (DoDI 7050.05) requires formal communication and coordination with the appropriate Government Centralized Organizations regarding all significant investigations. The Centralized Organizations are further defined in the Definitions section of this policy. The Defense Criminal Investigative Organizations (DCIO) are also directed to immediately notify the Defense Security Service of any investigation that develops evidence that would impact on DoD-cleared industrial facilities or personnel.

25.2.c. Effective and timely communication of information developed during DCIS investigations to affected Government entities and the various Department of Defense (DoD) components enables the Government to seek appropriate criminal, civil, contractual, and administrative remedies, as applicable by law or regulation.

25.2.d. Contractual remedies include correction of defects, denial of claims submitted by contractor, disallowance of contract costs, price reduction, cancellation of contract, refusal to accept nonconforming goods, termination of contract for default, and withholding of payments to contractor, or reducing fee or price for non-performance or unmet contractual requirements.

25.2.e. Administrative remedies include contract modifications; termination of contract; removal of contractor or subcontractor from Qualified Product List, Qualified Manufacturer's List, Qualified Suppliers List Government, or similar preferred Government source list; or suspension or debarment of contractor or contractor employees.

25.2.e.(1). Suspension and debarment actions are not punitive actions and no attempt should be made to use them to punish the contractor. Instead, they should be properly imposed to protect the Government's business interests. The issue is the present responsibility of a contractor or a person.

25.3 Security Clearance Suspensions and Revocations

25.3.a. DoD clearance adjudication is the evaluation of derogatory information contained in an investigation or other documents. A judgment concerning DoD security clearance eligibility is made by evaluating the information against the DoD Adjudicative Standards.

25.3.b. Adjudicative determinations for DoD contract employees, DoD civilian employees, and DoD military members are made by the DoD Consolidated Adjudication Facility (DoD-CAF), National Geospatial Agency (NGA), the Defense Intelligence Agency (DIA), and the National Security Agency (NSA). In addition, the Defense Security Service (DSS) may suspend clearances for DoD contract employees and contractor facilities. However, final adjudicative determination for contract employees and facilities is conducted by the DoD-CAF.

25.4. Definitions

25.4.a. Significant Investigation. Significant investigations, as defined in the DoDI 7050.05, are investigations involving allegations of procurement fraud, public corruption, bribery, gratuities, or conflicts of interest; all defective product, non-conforming product, counterfeit materiel, or product substitution investigations; and investigations otherwise determined to be significant by the cognizant agency official. The DCIS cognizant agency official is the Director, DCIS. Specifically, DCIS significant investigations may be associated to the corresponding case category codes defined in Special Agents Manual Chapter 28, “Investigative Reports.”

25.4.b. Remedies. Actions to achieve justice in any matter in which legal rights are involved. Actions that should be initiated by a commander or official having responsibility over a matter central to a significant procurement fraud case to protect DoD interests and to deter future incidents of fraudulent conduct. For more information on remedies, refer to DoDI 7050.05.

25.4.c. Centralized Organization. The centralized office within a Government entity or DoD Component designated to monitor and ensure the coordination of criminal, civil, administrative, and contractual remedies, to include suspension and debarment actions, for each significant investigation affecting the DoD Component, as defined in the DoDI 7050.05,. The Centralized Organizations are evolving entities.

25.4.d. Suspension. A discretionary action taken by a suspending official to temporarily disqualify a contractor or person from Government contracting, Government approved subcontracting, or participating in covered transactions. A contractor or person so disqualified is “suspended.”

25.4.e. Debarment. A discretionary action taken by a debarring official to exclude a contractor or person for a reasonable and specified period of time from participating in Government contracting, Government approved subcontracting, or covered transactions. A contractor or person so excluded is “debarred.”

25.4.f. Suspension & Debarment Official (SDO). An official within the Centralized Organization that makes present responsibility determinations, and decides whether or not to take administrative actions such as suspension or debarment. DCIS coordinates significant investigations with the SDOs of the impacted DoD components.

From this point forward, the term “Centralized Organization” will be referred to as the “Suspension & Debarment Officials - SDOs”

The most commonly used SDOs are listed in **Table 1.0** below. For the SDOs who are not listed below, contact the Coordination of Remedies Program Manager to obtain current contact and agency nomenclature information.

AGENCY	SUSPENSION & DEBARMENT OFFICIAL
U.S. Army	DIRECTOR, U.S. ARMY PROCUREMENT FRAUD DIVISION, JUDGE ADVOCATE GENERAL
U.S. Navy	GENERAL COUNSEL, U.S. NAVY ACQUISITION INTEGRITY OFFICE
U.S. Air Force	CHIEF, PROCUREMENT FRAUD REMEDIES PROGRAM, OFFICE OF GENERAL COUNSEL, U.S. AIR FORCE
Defense Logistics Agency (DLA)	GENERAL COUNSEL, DEFENSE LOGISTICS AGENCY
Department of Veterans Affairs	SUSPENSION & DEBARMENT COMMITTEE, RISK MANAGEMENT AND COMPLIANCE SERVICE, DEPARTMENT OF VETERANS AFFAIRS
Table 1.0 Commonly Used Suspension & Debarment Officials	

25.4.g. Defense Security Service. Under the DoDD 5105.42, the Defense Security Service (DSS) is the Cognizant Security Agency (CSA) to administer, implement, monitor, and oversee the National Industrial Security Program (NISP). In addition, DSS provides authorized counterintelligence services, and manages and operates the associated program-specific information technology systems. The DSS also supports DoD efforts to improve security programs and processes.

25.4.h. National Industrial Security Program. Executive Order 12829 established the NISP to ensure that cleared U.S. defense industry personnel safeguard the classified information in their possession while performing work on contracts, programs, bids, or research and development efforts. DSS administers the NISP on behalf of the DoD and other U.S. Government departments and agencies.

25.4.i. DoD-Consolidated Adjudication Facility. The DoD-Consolidated Adjudication Facility (DoD-CAF) determines security clearance eligibility of non-Intelligence Agency DoD personnel occupying sensitive positions or requiring access to classified material including Sensitive Compartmented Information (SCI). These determinations involve all military service members, applicants, civilian employees, consultants affiliated with DoD to include DoD personnel at the White House, and contractor personnel under the NISP. Additionally, with the assistance of DSS, the DoD-CAF renders final adjudicative determinations for employment suitability and Common Access Card (CAC) of DoD civilian employees, and fitness eligibility of non-cleared DoD contractors.

25.4.j. National Security. The term “national security,” for the purposes of security clearance suitability, is “the national defense and foreign relations of the United States,” as defined in DoD 5200.2-R, Paragraph DL1.1.16. Factors to consider when assessing risk to national security include the level of potential risk, seriousness of the subject’s alleged conduct, potential for coercion or blackmail of the subject, the individual’s level of access to sensitive information,

and the individual's level of influence over an organization. As these matters are not always clearly defined, DCIS personnel should consult with the DCIS National Security Program for guidance regarding specific cases.

25.4.k. Defense Criminal Investigative Organizations. The Defense Criminal Investigative Organizations (DCIOs) include the following investigative agencies: (1) Defense Criminal Investigative Service, (2) Army Criminal Investigation Command, (3) Naval Criminal Investigative Service, (4) Air Force Office of Special Investigations, and (5) Coast Guard Investigative Service.

25.5. Suspension

25.5.a. A suspension is for a temporary period of time, pending the completion of an investigation and any ensuing legal proceeding, unless previously terminated by the suspending official. If legal proceedings are not initiated within 12 months after the date of the suspension notice, the suspension must be terminated unless an Assistant Attorney General requests an extension. In such cases, the suspension may be extended for an additional 6 months; however, under no circumstances can a suspension be extended beyond 18 months unless legal proceedings were initiated during the initial 18 month period. Once a legal proceeding has been formally initiated (through an action such as an indictment or criminal complaint), a contractor may remain suspended until that legal proceeding is completed, including all appeals. Such proceedings are considered to be complete upon sentencing or acquittal.

25.5.b. The standard of evidence for a suspension is adequate evidence. This means the information must be sufficient to support the reasonable belief that the particular act or omission has occurred and that the contractor or person is responsible for the act or omission.

25.5.c. Indictment for any of the causes below constitutes adequate evidence for suspension. The suspending official may suspend a contractor or participant suspected, upon adequate evidence, of the following:

25.5.c.(1). commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing on a contract or covered transaction;

25.5.c.(2). violation of Federal or state antitrust statutes relating to the submission;

25.5.c.(3). commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, or receiving stolen property;

25.5.c.(4). violations of the Drug-Free Workplace Act of 1988 (Public Law 100-690);

25.5.c.(5). intentionally indicating that goods not made in the United States were made in the United States;

25.5.c.(6). commission of an unfair trade practice; or

25.5.c.(7). commission of any other offense indicating a lack of business integrity or business honesty that seriously and directly affects the present responsibility of a Government contractor or participant.

25.6. Debarment

25.6.a. A debarment is for a specified period of time commensurate with the seriousness of the acts. If a suspension precedes the debarment, the period of suspension is considered in determining the period of debarment. Generally, debarment should not exceed 3 years, except debarment for a violation of the provisions of the Drug-Free Workplace Act may be for a period not to exceed 5 years.

25.6.b. The standard of evidence for a debarment is preponderance of evidence. FAR Subpart 9.403. defines preponderance of evidence as “proof by information that, compared with that opposing it, leads to the conclusion that the fact at issue is more probably true than not.”

25.6.c. The debarring official may debar a contractor or participant for: (1) a criminal conviction or a civil judgment, (2) a violation of the terms of a Government contract or covered transaction, (3) a violation of the Drug-Free Workplace Act of 1988, or (4) any other cause so serious or compelling in nature that it affects the present responsibility of a Government contractor or participant.

25.6.c.(1). Debarment may occur upon criminal conviction or a civil judgment for the following:

25.6.c.(1).(a). commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing on a contract or covered transaction;

25.6.c.(1).(b). violation of Federal or state antitrust statutes relating to the submission of offers;

25.6.c.(1).(c). commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, tax evasion, or receiving stolen property;

25.6.c.(1).(d). intentionally indicating that goods not made in the United States were made in the United States; or

25.6.c.(1).(e). commission of any other offense indicating a lack of business integrity or business honesty that seriously and directly affects the present responsibility of a Government contractor or participant.

25.6.c.(2). Debarment may occur upon a serious violation of the terms of a Government contract or covered transaction such as the following:

25.6.c.(2).(a). willful failure to perform in accordance with the terms of one or more contracts or covered transactions;

25.6.c.(2).(b). a history of failure to perform or unsatisfactory performance on one or more contracts or covered transactions;

25.6.c.(2).(c). intentionally indicating that goods not made in the United States were made in the United States; or

25.6.c.(2).(d). commission of an unfair trade practice.

25.7. Reporting Requirements

25.7.a. Notification to the SDOs of Significant Investigations. DoDI 7050.05 requires all DCIOs to notify, in writing, the SDOs of all significant investigations.

25.7.a.(1) DCIS will provide timely notification to the affected SDO of all significant investigations in writing.

25.7.a.(2). The written notification will be conducted through a DoDI 7050.05 Notification Memorandum in accordance with procedures outlined in Attachment A.

25.7.a.(3). Exceptions to this notification requirement are further described in Attachment A.

25.7.a.(4). Make simultaneous presentations, whenever possible, of all fraud and corruption investigations to the criminal and civil sections of the appropriate United States Attorney's Office or the Criminal Division and the Civil Division, DOJ.

25.7.a.(5). Routinely discuss with the SDOs such issues as the status of significant investigations and their coordination with prosecution authorities.

25.7.a.(6). Provide prosecution authorities information on any adverse impact on a DoD mission, where such information also can be used in preparing a victim-impact statement for use in sentencing proceedings.

25.7.a.(7). For all significant investigations, share all available non-grand jury investigative information with the SDOs.

25.7.a.(7).(a). DCIOs are encouraged to use non-grand jury investigative techniques whenever possible to share non-grand jury investigative information with the SDOs, allowing use in civil, administrative, and contractual remedies

25.7.a.(7).(b). Grand jury investigative techniques (for example the use of grand jury testimony and grand jury subpoenas) should be used only when other investigative techniques have proven unsuccessful or are deemed inappropriate based upon specific circumstances associated with the investigation.

25.7.a.(8). Discuss regularly with the SDOs such issues as the status of significant investigations and their coordination with prosecution authorities. Documents summarizing the current status of the investigation, to include completed reports of investigation, will be provided to the SDOs in accordance with the established reporting requirements of DCIS.

25.7.a.(9). Immediately provide prosecution authorities information on any adverse impact on a DoD mission. Such information also can be used in preparing a victim-impact statement for use in sentencing proceedings.

25.7.a.(10). Gather at the earliest practical point in the investigation, and whenever possible without reliance on grand jury subpoenas, relevant information on responsible individuals and the organizational structure, finances, and contract history of DoD contractors or subcontractors under investigation for fraud or corruption related to procurement activities, in order to facilitate the criminal investigation. Compile any civil, contractual, or administrative remedies that may be taken.

25.7.b. Notification of a Suspected Defective Product. For all defective product, non-conforming product, counterfeit materiel, or product substitution investigations during which a serious hazard to health, safety, or operational readiness is identified, DCIS must notify, in writing, the appropriate SDO of the initiation of the investigation.

25.7.b.(1). The written notification will be conducted through a Suspected Defective Product Memorandum in accordance with procedures outlined in Attachment B.

25.7.b.(2). Exceptions to this notification requirement are further described in Attachment B.

25.7.b.(3). Continue to provide to the SDOs any information developed during the course of the investigation that indicates a suspect product has been, or might be, provided to the DoD.

25.7.c. Referral of Derogatory Information to the DSS and DoD-CAF. When a DCIS investigation identifies or develops credible information of derogatory information, which may have an immediate risk to national security, or the Government security clearance of an individual or an entity, then a referral to the DSS and the DoD-CAF shall be conducted.

25.7.c.(1). A referral to the DSS and DoD-CAF will be conducted in accordance with procedures outlined in Attachment B.

25.7.c.(2). Exceptions to this reporting requirement are further described in Attachment B.

25.8. SDO Duties. The SDO shall:

25.8.a review the notice of the investigation immediately after receiving it from the investigator to determine any potential safety or readiness issues indicated by the suspected fraud;

25.8.b. notify all appropriate safety, procurement, and program officials of the existence of the investigation, as long as prior coordination with DCIS and DOJ is conducted to ensure the disclosure of the investigation does not impact operational, agent, and public safety;

25.8.c. ensure the DoD Component provides DCIS with full testing support to completely identify the nonconforming or defective nature of the suspect products (The appropriate procurement program shall assume costs associated with testing);

25.8.d. prepare a comprehensive impact statement describing the adverse impact of the fraud on DoD programs for use in any criminal, civil, contractual, or administrative action related to the matter; and

25.8.e. ensure that, in all cases involving allegations affecting more than one DoD Component, the SDOs identify a Lead SDO.

25.8.e.(1). If the SDOs fail to identify a Lead SDO, the case agent will request through the Program Manager to coordinate with the Under Secretary of Defense for Acquisition, Technology, and Logistics to designate one of the SDOs to serve as the Lead SDO.

25.8.e.(2). The Lead SDO shall ensure that information on the fraud is provided to all other affected SDOs and determine whether non-DoD Government organizations are also affected, taking the lead for DoD in coordinating with those other Government organizations.

ATTACHMENTS

- A. Procedures for Notifying SDOs of Significant Investigations
- B. Reporting Derogatory Information to DSS and DoD-CAF

ATTACHMENT A

PROCEDURES FOR NOTIFYING SDOs OF SIGNIFICANT INVESTIGATIONS

Reporting Requirement (DoDI 7050.05 Notification)

The Resident Agent in Charge (RAC) must ensure the following SDO reporting requirements are performed for significant investigations within 90 days of case initiation.

1. The case agent completes a DoDI 7050.05 notification template labelled “A-1” under “Case File Resources” (an example of a completed template is labelled “A-2”). Both can be found at <https://intra.dodig.mil/inv/CoordinationRemedies/index.html>.
2. For a standard DoDI 7050.05 notification, the RAC reviews and digitally signs the completed notification then sends the notification to the DCIS Coordination of Remedies inbox for processing at DCIS.CoordinationOfRemedies@dodig.mil.
3. The DCIS Coordination of Remedies Program Manager (PM) forwards the DoDI 7050.05 notification to the SDOs, who are the addressed recipients in the notification, while courtesy copying the RAC and case agent.

Reporting Requirement (Suspected Defective Product Notification)

The RAC must ensure the following SDO reporting requirements are performed for investigations that meet the Suspected Defective Product Notification (SDPN) reporting criteria.

1. The case agent completes the SDPN template labelled “B-1” under “Case File Resources” (an example of a completed template is labelled “B-2”). Both can be found at <https://intra.dodig.mil/inv/CoordinationRemedies/index.html>.
 - 1a. If the case has **NOT** developed information to specifically identify the defective product information such as part numbers, stock numbers, or DoD nexus at the time of the notification, then a premature SDPN should be issued. For an example, see the template labelled “B-3” under “Case File Resources” located at <https://intra.dodig.mil/inv/CoordinationRemedies/index.html>.
 - 1b. If another agency previously issued a formal notification, Government Industry Data Exchange Program (GIDEP) alert, safety bulletin, a Defense Contract Management Agency (DCMA) corrective action report (CAR), or similar formal Government agency safety notification regarding the suspected defective products:
 - 1b(1). It is NOT necessary to issue a subsequent SDPN.
 - 1b(2). Obtain a copy of the previously issued GIDEP alert, safety bulletin, or similar formal Government agency safety notification and electronically upload into the CRIMS VCF using document type “NOTICE/DEFECTIVE PRODUCT,” no DCIS Form 1 is needed.
 - 1c. The RAC reviews and electronically sends the draft SDPN to the DCIS Coordination of Remedies inbox at DCIS.CoordinationOfRemedies@dodig.mil.

ATTACHMENT A

- 1d. The DCIS Product Substitution PM will review and forward the SDPN to the editor for editorial review. Once editorial review is completed, the SDPN will be sent to the DAIGI for Investigations for final signature.
- 1e. Once the SDPN is signed by the DAIGI, the DCIS Product Substitution PM will electronically send the signed SDPN to the SDOs, who are the addressed recipients in the SDPN, while courtesy copying the RAC and case agent.

Case File Documentation

The case agent will electronically file the following documents into the CRIMS Virtual Case File (VCF) under the “New Case Document” tab: Document (A) Final copy of the DoDI 7050.05 or SDPN memorandum, and Document (B) Copy of the e-mail notification that was sent to the Centralized Organization).

1. If the notification memorandum was related to a DoDI 7050.05 notification, select the CRIMS VCF document type, “**NOTICE/7050.05.**”
2. If the notification memorandum was related to a SDPN, select the CRIMS VCF document type, “**NOTICE/DEFECTIVE PRODUCT.**”
3. The DoDI 7050.05 notification and the SDPN is a standalone document in the official case file; a DCIS Form 1 is NOT needed. However, a hardcopy of both Documents (A) and (B) must be retained in the working case file.

Exceptions to the DoDI 7050.05 Reporting Requirements

The intent of the DoDI 7050.05 reporting requirements is to enable the sharing of information concerning procurement fraud and public corruption at the earliest possible moment, with the SDO, to permit contractual recoveries within applicable appropriations law restrictions, while balancing the need for agent and operational safety.

To ensure operational safety and prevent the compromise of ongoing criminal or administrative investigations, there are instances where the DoDI 7050.05 and the SDPN requirements are protected and in some instances not warranted. These instances include the following.

1. If another Government agency already notified an appropriate SDO regarding the significant investigation, then a DoDI 7050.05 notification is not required.
 - 1a. However, the case agent will obtain a copy of the Government agency notification for example a copy of the case initiation report distribution line indicating the SDO as a recipient of the report, any e-mail correspondence to the SDO, or similar written correspondence to the SDO, and upload this correspondence into the CRIMS VCF using document type, “**NOTICE/7050.05.**”

ATTACHMENT A

- 1b. A DCIS Form-1 is not needed. However, a hardcopy of the written correspondence must be retained in the working case file.
2. If the significant investigation involves an ongoing undercover operation or where such notice would reveal sensitive law enforcement sources and methods utilized, then a DoDI 7050.05 notification is not required.
 3. If the notification will disclose information obtained through restricted means, which restricts or prohibits further disclosure of the information, to include but not limited to: Grand Jury, *Qui Tam*, consensual intercepts, court sealed documents, Bank Secrecy Act information, undercover operations, mail covers, or any DOJ provisions, then this information **MAY NOT** be disclosed until such information is unsealed or otherwise made public. This restricted disclosure is accomplished by indicating “**NOT REPORTABLE**” within the DoDI 7050.05 notification or SDPN. An example of non-reportable information is prescribed in the example labelled “A-3,” located in <https://intra.dodig.mil/inv/CoordinationRemedies/index.html>, under “Case File Resources”.

ATTACHMENT B

REPORTING DEROGATORY INFORMATION TO DSS and DoD-CAF

This appendix provides guidance for follow-on reporting of derogatory information to the Defense Security Service (DSS)/DoD-Consolidated Adjudication Facility (DoD-CAF) when a DCIS investigation identifies credible information¹ that may impact an individual's and/or company's eligibility for a security clearance.

Initial Reporting Requirement (DCII)

To satisfy the requirement set forth in DoD 5200.2-R to report derogatory information concerning individuals and/or companies eligible for a security clearance, DCIS expeditiously reports such information regarding subjects of investigations via the Defense Central Index of Investigations (DCII) in accordance with SAM Chapter 50. The DCII is a centralized database that contains identifying information and security clearance data utilized by security and investigative agencies in the DoD, as well as selected other Federal agencies, to determine security clearance status and the existence or physical location of criminal and personnel security investigative files.

Follow-on Reporting Requirements (DSS/DoD-CAF)

Follow-on reporting to the DSS/DoD-CAF shall be conducted, as required by DoDI 7050.05, upon the occurrence of each of the following events.

1. **Significant Incident Reports.** When a significant incident occurs, as defined in SAM Chapter 28, the first significant incident, per subject, pertaining to derogatory information shall be timely reported to the DSS/DoD-CAF. Subsequent to the first significant incident per subject, any sentencing incidents, civil settlements, and suspension and debarment actions should be timely reported to the DSS/DoD-CAF using the Referral Procedures outlined below. (Multiple significant incidents may be reported on one DSS/DoD-CAF referral if the incidents occur within 30 days of one another.)
2. **Cases Prepared for Closure or Suspense.** When cases are prepared for case closure or suspense, and if the disposition code is one of the following listed in Table 1.0, then the derogatory information contained therein relating to the suspects of the case that has not been previously reported, shall be reported to the DSS/DoD-CAF prior to closing or suspending using the Referral Procedures outlined below.

¹ SAM Chapter 50, Paragraph 50.8 Subject Reporting Policy, defines the term "credible information" as information disclosed or obtained by a criminal investigator that, considering the source and nature of the information and the totality of the circumstances, is sufficiently believable to lead a trained criminal investigator to presume that the fact or facts in question are true.

ATTACHMENT B

TABLE 1.0	
DISPOSITION CODE	DCIS CASE DISPOSITION CODE DESCRIPTIONS
(b)(7)(E)	DECLINATION - Prosecution declined and no administrative action taken
	FINISHED - Culpability established and at least 1 (or more) subject(s) adjudicated; Administrative action taken
	SUSPENSE - ROI completed; awaiting adjudicative decision/response

3. Immediate Risk to National Security. If at any time during an investigation, a DCIS RAC determines that derogatory information about an individual and/or company indicates the existence of an immediate risk to national security², then the derogatory information shall be expeditiously reported to the DSS/DoD-CAF using the Referral Procedures outlined below.

Reporting Requirement (DSS/DoD-CAF Referral)

The RAC shall notify DSS/DoD-CAF of the derogatory information with a formal memorandum and ensure the following actions are performed.

1. The case agent completes the DSS/DoD-CAF referral template labelled “C-1,” located in <https://intra.dodig.mil/inv/CoordinationRemedies/index.html>, under “Case File Resources.”
2. The RAC reviews and digitally signs the completed referral and electronically sends the notification to the DCIS Coordination of Remedies inbox for processing; DCIS.CoordinationOfRemedies@dodig.mil.
3. The Coordination of Remedies Program Manager (PM) will forward the DSS/DoD-CAF referral to the DSS/DoD-CAF Headquarter inbox, while courtesy copying the RAC and case agent.
4. The case agent will upload the e-mail notification into the CRIMS Virtual Case File (VCF) under the “Case File” tab, and select the CRIMS VCF document type, “NOTICE/DOD-CAF (ROUTINE).”
5. This notification memorandum is a standalone document in the official case file; a DCIS Form 1 is not needed. However, a hardcopy of both Document (A), Final copy of the DSS/DoD-CAF Notification, and Document (B), copy of the e-mail notification sent to the DSS/DoD-CAF must be retained in the working case file.

² The term “national security”, for the purposes of security clearance suitability, is “the national defense and foreign relations of the United States”, as defined in the DoD 5200.2-R, Paragraph DL1.1.16. Factors to consider when assessing risk to national security include the level of potential risk to national security, seriousness of the subject’s alleged conduct, potential for coercion or blackmail of the subject, the individual’s level of access to sensitive information, and/or the individual’s level of influence over an organization. As these matters are not always clearly defined, DCIS personnel should consult with the DCIS National Security Program for guidance regarding specific cases.

ATTACHMENT B

Exceptions to the DSS/DoD-CAF Reporting Requirements:

If a DCIS RAC determines the derogatory information of the suspects was obtained through restricted means, which restricts or prohibits further disclosure of the information, to include but not limited to: (1) Grand Jury, (2) sealed *Qui Tam* litigation, (3) consensual intercepts, (4) court sealed documents, (5) Bank Secrecy Act information, (6) undercover operations, (7) mail covers, or (8) any DOJ provisions, then this information **MAY NOT** be disclosed to the DSS/DoD-CAF until such information is unsealed or otherwise made public. This justification for withholding derogatory information to DSS/DoD-CAF will be documented in a memorandum using the format prescribed in the template labelled “C-3,” and ensure the following actions are performed.

1. The case agent should issue a DSS/DoD-CAF withholding of information memorandum as prescribed in the example labelled “C-3,” under “Case File Resources,” located in <https://intra.dodig.mil/inv/CoordinationRemedies/index.html>.
2. The RAC reviews and digitally signs the DSS/DoD-CAF withholding of information memorandum.
3. Case File Documentation. The case agent will electronically file DSS/DoD-CAF withholding memorandum into the CRIMS VCF under the “Case File” tab, and select the CRIMS VCF document type, “NOTICE/DOD-CAF (WITHHOLDING OF INFORMATION).”
4. This internal memorandum is a standalone document in the official case file; a DCIS Form 1 is not needed. However, a hardcopy of the internal memorandum, must be retained in the working case file.
5. If at any time during the investigation the derogatory information of the suspects are unsealed or made public, the RAC must follow the procedures contained in the “Follow-on Reporting Requirements (DSS/DoD-CAF)” section of this attachment to ensure the appropriate DSS/DoD-CAF notification has occurred.

CHAPTER 28

INVESTIGATIVE REPORTS

<u>Contents</u>	<u>Section</u>
General	28.1.
Case Reporting System	28.2.
Case Number	28.3.
Report Dates	28.4.
Titling of Suspects	28.5.
Document Types/Formats	28.6.
Special Reporting Requirements	28.7.
Exhibits/Attachments	28.8.
Distribution	28.9.
Use of the Form 1 for Case Initiations	28.10.
Use of the Form 1 for Investigative Projects	28.11.
Use of the Form 1 for Operational Purposes	28.12.
Use of the Form 1 for Lead Requests	28.13.
Use of the Form 1 for Requests for Other Types of Operational Support	28.14.
Use of the Form 1 for Case Summary–Updates	28.15.
Use of the Form 1 for Reporting Significant Incidents	28.16.
Use of the Form 1 for Reports of Investigation	28.17.
Use of the Form 1 for Information Reports	28.18.
DoD OIG Audit Coordination Memorandum	28.19.
Coordination of Remedies Reporting Requirements	28.20.
Other Required Reporting	28.21.
Case Review Requirements	28.22.
Case Closing Actions	28.23.

28.1. General

28.1.a. This chapter presents policy and guidance on preparing Defense Criminal Investigative Service (DCIS) investigative reports. The procedures in this chapter apply to DCIS Headquarters and all DCIS field offices (FO), resident agencies (RA), and posts of duty (POD).

28.1.b. Investigative reports are written to record information gathered during an investigative activity, such as an interview, record review, search and arrest warrants, or surveillance. Investigative reports will not contain the report writer's conclusions, recommendations, or judgments.

28.1.c. **Approval.** Supervisory approval is required on all DCIS investigative reports. All investigative reports will contain a "Prepared by" block containing the name and signature of the report writer and an "Approved by" block containing the name and signature of the report writer's immediate supervisor or designee. It is recommended that all DCIS investigative reports

be digitally signed; however, signing these reports manually is not prohibited. The final, signed reports are to be maintained in the official case file. Once the signature blocks are signed by both parties, the report is an official document and becomes part of the official case file. NOTE: In some instances it may become necessary to amend or correct a report once it has been signed. This will be done by preparing a supplemental report. **The original report will not be replaced or destroyed.**

28.1.d. Special agents (SAs) must ensure that investigative reports meet the highest standards of integrity, accuracy, and objectivity.

28.1.e. The word “exhibit” will describe any document appended to a Report of Investigation (ROI). The word “attachment” will describe a document appended to any other investigative report, such as a DCIS Form 1.

28.1.f. All investigative reports, exhibits, and attachments will be retained by the office of primary responsibility (OPR) in the official case files. The OPR is defined as the office where the lead agent conducting the investigation is assigned. The term “official case file” hereinafter includes the hard copy case file and Case Reporting and Information Management System (CRIMS) Virtual Case File (VCF). Special Agents Manual (SAM) Chapter 50, “Case Reporting and Information Management System,” contains information on VCF requirements. NOTE: Certain documents will not be uploaded into the VCF when they contain sensitive methods or sensitive investigative techniques with restricted dissemination, such as grand jury information or undercover techniques. At the Special Agent in Charge’s (SAC) discretion, the official case files for offices without clerical support may be maintained in the FO or RA. Hard copy case files will be maintained in accordance with SAM Chapter 42, “Investigative Records Management.”

28.1.g. If an attachment or exhibit to a DCIS report is considered too voluminous to be placed in the official case file or cannot be scanned electronically, it will be maintained by the case agent until the investigation is closed. If the documents are not attached to the hard copy report or scanned into the VCF, the following statement should be included in the narrative of the Form 1 or ROI: “Due to the voluminous nature, the attachments will not be appended to this report but will be maintained by the case agent.” NOTE: A copy of the associated Form 1 will be maintained with these documents. Also, see paragraph 28.23. for case closing actions regarding the handling of attachments or exhibits maintained outside of the official case file.

28.1.h. All DCIS investigative reports are prepared on a DCIS Form 1, using the Times New Roman font, size 12, on the letterhead of the associated FO, RA, or POD, and all paragraphs of the narrative section will be aligned with the left margin (“align left”). Attachment A is an example of a generic Form 1. However, certain relevant case-related reports and documents generated by outside agencies that stand on their own merit, such as FBI Forms 302, AFOSI Forms 40, and other joint agency ROIs, do not require the preparation of a cover Form 1 and will be maintained in the official case file. In a joint investigation with another agency, copies of the joint agency’s reports are regularly received. Copies of joint agencies’

reports will be retained in the official case file. Dissemination of an outside agency report is prohibited without permission from that agency. NOTE: Reports received from joint investigative agencies should also be uploaded in the VCF unless the authoring agency's policy expressly prohibits this.

28.1.i. Special agents shall disclose exculpatory evidence discovered during investigations to the assigned prosecutor and any legal authorities deemed appropriate. This information will be documented and maintained in the official case file. See SAM Chapter 1, "Organization, Mission, Jurisdiction, and Authorities," for further guidance on the disclosure of exculpatory evidence.

28.1.j. In CRIMS, the term "subject" refers collectively to persons or entities associated with investigations, such as suspects, persons of interest, victims, and witnesses. For consistency, the term "suspect," formally "subject" in previous publications of this chapter, will now be used to refer to the person or entity suspected of wrongdoing. NOTE: As of May 2017, the use of the term "suspect" is solely used in this chapter and SAM Chapter 50, "Case Reporting and Information Management System (CRIMS)." All other SAM chapters will continue to use the term "subject" until such time that they undergo revision. The term "suspect" will be incorporated into each SAM chapter at the time of its next revision.

28.2. Case Reporting System

28.2.a. An investigation will be initiated when specific credible information is developed that an individual or entity may have committed a criminal, civil, or administrative violation that has a direct financial harm to DoD or the violation impacts DoD components, programs, personnel, or property. All information obtained by or reported to DCIS that indicates a potential violation of law or regulation will be evaluated and documented either by a Case Initiation Report (CIR), Information Report (IR), or Information Report/Referred. SACs are authorized to initiate investigations within the geographic area of responsibility (AOR) to which the SAC is assigned. The authority of the SAC to initiate investigations stems from the overall authority and responsibility vested in the SAC by the Deputy Inspector General for Investigations (DIG-INV). The SAC may delegate the authority to initiate investigations to Assistant Special Agents in Charge (ASAC) and Resident Agents in Charge (RAC). The Deputy Assistant Inspector General for Investigations (DAIGI), Investigative Operations Directorate (Investigative Operations), in conjunction with the Assistant Inspector General for Investigations (AIGI), Investigative Operations, has the authority to direct the initiation, closing, or reopening of any investigation as deemed necessary. This action will not be taken without prior coordination with the SAC of the affected investigation and, when applicable, the DAIGI, International Operations Directorate (International Operations). Attachment B is an example of a generic CIR.

(b)(7)(E)

(b)(7)(E)

28.2.b.(1). **International Investigations and Subjects.** In any instance where an investigative target is located outside the United States, whether it be an ongoing investigation or an initial referral, the case will be immediately coordinated with the RAC of the International Resident Agency and the Program Manager for International Affairs. For initial referrals, such coordination will occur prior to obtaining a unique identifier (UID) and the coordination will be documented in the CIR. In ongoing investigations or undercover operations, the coordination will be documented in a separate Form 1. The affected RACs will come to an agreement as to which office will work the investigation or if it will be worked jointly between the impacted offices. The term "outside the United States" includes all foreign U.S. possessions such as Puerto Rico and Guam, but excludes the non-contiguous U.S. states, Alaska and Hawaii. Should a dispute arise that cannot be resolved at the RAC level, the matter will be elevated for resolution to the SAC or ASAC level of the affected offices. These disputes should only be referred to the DAIGIs for Investigative Operations and International Operations if they cannot be resolved at the field level. Additionally, all investigations where the alleged crime or contract performance occurred outside of the United States will be coordinated with the Program Manager for International Affairs upon case initiation.

(b)(7)(E)

(b)(7)(E)

28.2.e. Reports in CRIMS are official documents that are subject to the records retention provisions of Federal law. Once a CIR is posted online in the CRIMS VCF, it cannot be modified or removed without the approval of the associated SAC. The SAC may delegate approval authority to the ASAC or RAC. If a CIR needs to be modified or corrected after being posted, seek guidance from the Internal Operations Directorate (Internal Operations) on how it should be posted in CRIMS. The first sentence of the narrative of the CIR should state the reasons the report was corrected. Attachment C is an example of a corrected CIR. If any other online report in CRIMS must be corrected or modified, for example IRs, ROIs, or Case Summary–Updates, a supplemental report will be created and posted in CRIMS. Similar to the CIR, the first sentence of the narrative of other online reports (such as IRs, ROIs, and Case Summary–Updates) must state the reasons why the original report was corrected or modified. Both the original and supplemental reports will be maintained in the hard copy case file and CRIMS VCF. If another type of Form 1 must be corrected, a supplemental report will be created and maintained in the hard copy case file and posted in CRIMS VCF. Attachment D is an example of a Supplemental Information Form 1.

28.2.f. On a joint investigation or task force, if the joint agency upgrades previously unclassified information to classified and the case agent has already posted the information in CRIMS, the FO must (1) obtain and fax or e-mail Internal Operations a copy of a letter from the joint agency stating its classification authority and (2) submit a request by the SAC or his/her designee for the removal of the classified information from CRIMS. The SAC's request and the letter from the joint agency can be sent via e-mail. The original letter will be filed in the official case file. Upon receipt of the letter, Internal Operations will coordinate with the FO to comply with the request to remove the classified information from CRIMS.

28.2.g. **Case Transfer.** Transfer of case control may be necessary when an OPR determines either the majority of the investigative activity or the established venue for prosecution lies in the geographic area of another office or the case involves Special Access or Sensitive Compartmented Information. Coordination must be made with the receiving office before transferring control of a case. The OPR transferring the case must verify all data entered into CRIMS is correct and the most recent 90-day Case Summary–Update and investigative activity to date has been uploaded into the VCF before the transfer. If the receiving office agrees to accept the case transfer, the receiving office must send Internal Operations an e-mail requesting the reassignment of the case in CRIMS to the new OPR and case agent. The e-mail

should be succinct and contain no extraneous or personal comments. The transferring office will send all original case-related materials, to include the transfer of evidence, to the receiving office. Upon the transfer of a case from one office to another, future Forms 1 will reflect the assuming office's OPR code in the CN. Attachments GG and HH are examples of Case Transfer Forms 1. See SAM Chapter 50 for further guidance on transferring cases in CRIMS.

28.2.h. Case Reassignment. When a case is reassigned to a different agent within the same office, the RAC will update CRIMS to reflect the change of case agents. Attachment II is an example of a Case Reassignment Form 1. See SAM Chapter 50 for further guidance on reassigning cases in CRIMS.

28.3. Case Number

28.3.a. All investigative reports require a Case Number (CN). The CN is obtained by the OPR when an investigation is initiated or an IR is prepared. SAM Chapter 50 contains information on CRIMS requirements. The CN (for example, 2014000010- (b)(7)(E) for DCIS reports consists of the three elements described below.

28.3.a.(1). Unique Identifier. The system-generated 10-digit identifier automatically assigned by CRIMS to the selected case record when it is created, such as 2014000010 in the above example. The first four digits indicate the fiscal year in which the CDP was initially created in CRIMS. CDPs are the initial entries that lead to a CIR or an IR. The next six digits indicate a sequential number assignment within CRIMS relative to the specified fiscal year, beginning with 000001 and continuing through 999999. Once assigned to an investigative effort, a UID cannot be changed.

(b)(7)(E)

(b)(7)(E)

28.4. Report Dates. The dates of all reports, without exception, will conform to the following.

28.4.a. **CIRs.** The date of the CIR will be the date the report was prepared by the reporting agent. However, the official case opening date for the investigation will be the date the investigation was approved by the supervisor in CRIMS.

28.4.b. **IRs.** The date of an IR will be the date the report was prepared by the reporting agent. However, the official date for the IR will be the date the report is approved for closure by the supervisor in CRIMS.

28.4.c. **Case Summary–Updates.** The date of the report will be the date that conforms to the reporting cycle for the reporting period.

28.4.d. **ROIs and Case Terminations.** The date of the ROI will be the date the report was prepared by the reporting agent. However, the closed date for the case will be the date the ROI or Case Termination is approved for closure by the supervisor in CRIMS, except for prosecutorial ROIs.

28.4.e. **All Other Forms 1.** The date of the document will be the date the report was prepared by the reporting agent.

(b)(7)(E)

28.6. Document Types/Formats

28.6.a. **General.** The Form 1 is used to report all operational and case-related activities, to include summary updates, information, and intelligence. All DCIS investigative reports are prepared using the Times New Roman font, size 12, on the letterhead of the associated FO, RA, or POD in the format of the standard Form 1. Paragraphs in DCIS reports are not numbered, except the narrative portion of ROIs. All Forms 1 will be posted online in CRIMS, except those with restrictions. See SAM Chapter 50 for further guidance on posting online reports.

28.6.b. **Acronyms, Abbreviations, and Grammar.** The title “special agent” will be abbreviated as “SA” in all reports. States will be abbreviated using the two-letter postal format, except when referred to as an entity, for example Eastern District of Missouri, St. Louis, MO. United States will be abbreviated as U.S. The use of other abbreviations and acronyms, including those for Government agencies and business entities, is acceptable after the full word has been spelled out on its first appearance in the body of the report followed by its abbreviation or acronym in parentheses, for example the Internal Revenue Service (IRS), General Electric Company (GE), General Motors Corporation (GMC), or Defense Contract Management Agency (DCMA). Attachment I is a reference of commonly used acronyms and abbreviations. The grammar and style of DCIS documents will follow the direction established in the DoD OIG “Editorial Guide and Reminders for DoD OIG Documents.” The current Guide can be found on the DoD OIG Intranet at <https://intra.dodig.mil/fo/EA/InternalComm/toolkit/EditorialGuideReminders.pdf>.

28.6.c. **Report Title.** The report title will be the initial entry of the first paragraph of the narrative section of the Form 1, typed in all capital bold letters and underlined, will identify the title/type of document for which the Form 1 is being used, such as Case Initiation, Case Summary–Update, Witness Interview, or Records Review. The initial entry should be sufficiently specific to allow a reader to distinguish the intent of each Form 1. Attachment J is a list of suggested Form 1 report titles.

28.6.d. **Special Markings on Forms 1 and Sensitive Investigative Techniques.** All Forms 1 must display the “For Official Use Only–Law Enforcement Sensitive” (FOUO–LES) markings, pursuant to guidance issued by the Deputy Undersecretary of Defense for Intelligence relative to DoD Instruction 5200.01, “DoD Information Security Program and Protection of Sensitive Compartmented Information,” Change 1, June 13, 2011, and DoD Manual 5200.01, Volume 4, “DoD Information Security Program: Controlled Unclassified Information,” February 24, 2012. The FOUO–LES designation is used within DoD to identify information that was compiled for law enforcement purposes and requires special handling to protect legitimate

Government interests. Specifically, this refers to information pertaining to enforcement proceedings; personal privacy matters, such as Privacy Act information, confidential informants, and techniques or procedures for law enforcement investigations or prosecutions; and guidelines for law enforcement investigations when disclosure of such guidelines could reasonably be expected to risk circumvention of the law or jeopardize the life or physical safety of any individual, including law enforcement personnel. The FOUO–LES marking on unclassified documents containing such information should be placed at the bottom of the front cover (if there is one), the title page (if there is one), and the outside of the back cover (if there is one). Each page containing FOUO–LES information shall be appropriately marked at the bottom.

28.6.d.(1). **Classified Material.** If any DCIS report contains classified material, it will be properly marked in accordance with DoD Manual 5200.01, “DoD Information Security Program: Overview, Classification, and Declassification; DoD 5200.1-PH, “DoD Guide to Marking Classified Documents,” April 1, 1997; and IGDINST 5200.1, “Information Security Program,” August 31, 2007. **Under no circumstances will the official unclassified case file contain classified information, and under no circumstances will classified documents be uploaded to CRIMS.** Contact the Program Manager, Sensitive Investigations Program, for further guidance regarding the preparation, marking, storage, accountability, reproduction, transmission, transportation, or disposal of any classified case documents.

(b)(7)(E)

(b)(7)(E)

28.6.e. Prepared By, Approved By, and Distribution. All investigative reports will contain a “Prepared by” block containing the report writer’s name, office code (for example, 50LA), and signature, and an “Approved by” block containing the name of the report writer’s immediate supervisor, office code, and signature. Reports requiring dissemination will contain a distribution entry (such as DISTR) in the lower left-hand portion of the document and will include the applicable DCIS office code, external organization, or both. The Prepared by/Approval/Distribution block will always be on the bottom of the last page of the document. If the document is an ROI, the Distribution block will be listed at the bottom of the ROI cover page and the Prepared by/Approval block should be on the last page of the ROI. NOTE: Digital signatures are recommended. The format will be as follows:

Prepared by: John A. Doe, 50LA

Approved by: James R. Smith, 50LA

<Digitally sign above the line.>

<Digitally sign above the line.>

DISTR: 20FO/HHS/DHA

28.7. Special Reporting Requirements

28.7.a. Special Interest Case (SIC) Factors. When the circumstances of an investigation meet the criteria specified below, only CIR, CIR - Corrected, Case Summary–Update, or IR Forms 1, not ROIs, will contain SIC factors. This is required, either at case initiation or at some future point in the investigation. Appropriate CRIMS entries will be made by the OPR and the special interest factors will be included for the duration of the investigation or until the SIC designation is no longer applicable. NOTE: Reports no longer include banners or the statement “SPECIAL INTEREST CASE.” If an investigation is a SIC, the following special interest factors must be listed in the “Special Interest Factors” section of all CIR or Case Summary–Updates. If any of the categories for a SIC are met after an investigation has been initiated, then the next Case Summary–Update will reflect this information, to include the addition of the applicable “Special Interest Factors” section of the report. For IRs, SIC factors must be identified in the opening paragraph of the “Narrative” section of the applicable IR. Attachment K is a listing of the Special Interest Case Factors.

28.7.a.(1). **Suspected Defective Product.** Any investigation involving the issuance of a Notice of Suspected Defective Product Memorandum (formerly known as Safety Alert), Government - Industry Data Exchange Program (GIDEP) alert, or the equivalent safety notification regardless of who issued the notice should be identified as a SIC.

28.7.a.(2). **American Recovery and Reinvestment Act.** Any investigation into alleged fraud, waste, or abuse involving funds made available to DoD under the “American Recovery and Reinvestment Act of 2009” (Recovery Act) should be identified as a SIC. Any referral received from the Recovery Act and Transparency Board (RATB) must include the RATB tracking number. NOTE: The DoD Hotline is tracking RATB referrals and subsequently assigning DoD Hotline numbers to them. If this occurs, the Hotline tracking number is also required to be added as an agency tracking number in the “Referral Sources” section of the CIR, Case Summary–Update, or IR Forms 1.

28.7.a.(3). **Overseas Contingency Operations (OCO).** OCO includes any military operation occurring outside the U.S. that is either designated by the Secretary of Defense as a contingency operation or becomes a contingency operation as a matter of law (Title 10 United States Code, Section 101(a)(13)).” OCO includes, but is not limited to, Operation Iraqi Freedom, Operation New Dawn, Operation Enduring Freedom (OEF) - Afghanistan, OEF - Horn of Africa, and OEF - Philippines. Coordination should be made with the International Affairs Program for any investigation relating to OCO activity.

28.7.a.(4). **Congressional Inquiry.** Any investigation involving a formal inquiry from a congressional office and assigned a tracking number by the DoD OIG Office of Legislative Affairs and Communications (OLAC) should be identified as a “Congressional Inquiry.”

28.7.a.(5). **Small Business Innovative Research/Small Business Technology Transfer.** Any investigation involving fraud impacting the Small Business Innovative Research (SBIR) or Small Business Technology Transfer (STTR) programs should be identified as a “SBIR/STTR.”

28.7.a.(6). **Trafficking in Persons.** Any investigation involving trafficking in persons that falls within the investigative purview of DCIS should be identified as “Trafficking in Persons.” Coordination should be made with the International Affairs Program for the latest guidance on investigations involving trafficking in persons.

28.7.a.(7). **Sensitive Investigations.** Any investigation identified as a classified investigation or any investigation (classified or unclassified) involving programs or personnel administered by the DoD Intelligence Community, regardless of the case category, should be identified as a “Sensitive Investigation.” See SAM Chapter 2, “Sensitive Investigations Program,” for guidance regarding case openings and the preparation of investigative reports concerning sensitive investigations.

(b)(7)(E)

28.7.a.(9). **Multiple SIC Factors.** If an investigation involves multiple SIC factors, the CIR, Case Summary–Update, or IR Forms 1 will depict all applicable SIC criteria.

28.7.b. **Referral Sources.** DCIS will receive referrals from various sources. Each referral source should be reflected in the “Referral Sources” section of the CIR and Case Summary–Updates. There may be multiple referral sources for an investigation, and they should be listed separately on the applicable Form 1. For IRs, referral sources must be identified in the opening paragraph of the “Narrative” section of the applicable IR. All referral sources should be entered separately in CRIMS.

28.7.b.(1). The field will also receive numbered referrals from sources which are tracked by DCIS Headquarters. These referrals include, but are not limited to, DoD Hotline, DoD OIG Office of the Deputy Inspector General for Auditing (ODIG-AUD), Defense Contract Audit Agency, Contractor Disclosures, Department of Justice (DOJ) *qui tam* lawsuits, Defense Health Agency, and the Defense Finance and Accounting Service. The CIR and Case Summary–Updates for any investigation involving a referral, as well as those referrals tracked by DCIS Headquarters, must include the entity’s names and the corresponding tracking numbers\), if applicable, in the “Referral Sources” section of the applicable Form 1. For IRs, the referral sources for these types of referrals must be identified in the opening paragraph of the “Narrative” section, to include the entity’s names and the corresponding tracking numbers, if applicable. NOTE: If a FO reviews a DCIS Headquarters referral and determines it should have been referred to a different DCIS FO at the onset, the receiving FO must immediately contact the appropriate desk officer/program manager. If DCIS Headquarters concurs with redirecting the referral to another DCIS FO, the FO will update CRIMS by reassigning the CDP to the appropriate DCIS FO. See SAM Chapter 50 for guidance on reassigning CDPs. Otherwise, the FO should perform the preliminary review/inquiry and prepare a CIR, IR, or IR/Referred.

28.7.b.(2). Should a referral be received after the case is initiated, the agency’s tracking number, if applicable, shall be reflected in the next Case Summary–Update and entered into CRIMS, to include adding the applicable agency’s tracking number in the “Referral Sources” section of the report. As appropriate, referral sources should be included in the

“Distribution” section of all CIR, Case Summary, Case Summary–Updates, and IRs. See Attachment M for examples of common referral sources and agency tracking numbers.

(b)(7)(E)

(b)(7)(E)

28.8. Exhibits/Attachments

28.8.a. **General.** Documents referred to as exhibits or attachments in the text of an investigative report will be listed in order at the end of the text, and aligned to the left margin. Exhibits or attachments will be numbered if more than one exhibit or attachment is appended. When there are numerous exhibits/attachments, tabs or pages (marked) will be used to delineate them. All exhibits or attachments will be filed with the original case file, unless otherwise specifically noted in the report. See the following examples:

28.8.a.(1). Attachment:
Copy of Indictment, dated June 25, 2008

28.8.a.(2). Attachments:
1. DCAA Form 2000, dated January 1, 2008
2. Copy of Invoice No. 3211

28.9. Distribution

28.9.a. **General.** Certain DCIS reports may require dissemination to other DCIS offices, Military Criminal Investigative Organizations (MCIO), victim agencies, other DoD Components, or other agencies. The recipient (the DCIS office code or non-DCIS agency designation) will be listed in the lower left corner of the document following the entry "DISTR." Original reports and attachments will be retained in the official file and should not be sent to DCIS HQ, as they can be accessed in CRIMS. All distribution addressees will receive copies of all exhibits or attachments, unless otherwise stated. For any addressee receiving less than complete distribution, either the exhibits/attachments to be provided or the exhibits/attachments not provided (whichever is fewer) should be noted next to the designated recipient, such as DCMA Syracuse Fraud Counsel (w/out Attachments) in the list of exhibits/attachments or the distribution block. Case agents are responsible for ensuring DCIS reports are provided to the appropriate recipients. Non-availability of the case agent will not delay dissemination of reports; the immediate supervisor will ensure timely dissemination of reports is made if the case agent is unavailable. Distribution of DCIS reports via e-mail outside the DoD OIG network should be sent securely with encryption. Any reports sent in draft form should also be encrypted before being sent to outside agencies and must clearly display "draft" markings on all pages.

28.9.b. **Distribution Codes.** Any DCIS document (except ROIs) requiring dissemination will contain the applicable code, designation, or name of the recipient. The acronym for recipients can also be used (for example, FBI – Atlanta/USAO (AUSA Clifford)/DCMA – Atlanta /200R).

28.9.c. **Restricted Dissemination.** Some special circumstances may adversely affect the successful completion of an investigation and may warrant strict internal DCIS or DoD OIG distribution. A field SAC or DAIGI, as well as the appropriate ASAC or RAC, has the authority to restrict dissemination of reports with the exception of those that describe covert operations, grand jury, or source information, which are already restricted. When restricted dissemination is approved, the reports will have an entry above any other special report warning statement. The entry will appear in boldface, upper case letters, underlined, and aligned to the left margin as set forth below.

DISSEMINATION OF THIS REPORT HAS BEEN RESTRICTED BY DCIS

28.9.d. **Grand Jury Material.** Grand jury material will not be distributed to any person not on the grand jury 6(e) list. Also, grand jury information will not be posted online. No

reference to grand jury information or material should be referenced in any report outside the official grand jury file. A document that contains grand jury information will be placed in the official grand jury file and clearly marked as follows:

**GRAND JURY MATERIAL - DISSEMINATE ONLY PURSUANT TO
RULE 6e(3), FEDERAL RULES OF CRIMINAL PROCEDURE**

28.9.d.(1). A preprinted stamp or sticker containing the above warning may be used. If typed rather than stamped on the Form 1, the entry must be in boldface, upper case letters, underlined, and aligned to the left margin above the report title or, if applicable, any special report warning statement. For example:

**GRAND JURY MATERIAL - DISSEMINATE ONLY PURSUANT TO
RULE 6e(3), FEDERAL RULES OF CRIMINAL PROCEDURE**

28.9.d.(2). Forms 1 that have grand jury material as an exhibit/attachment will be marked with the grand jury warning as stated above. The Form 1 and the material will be placed in the grand jury file. Further guidance concerning grand jury information is contained in SAM Chapter 15.

28.9.d.(3). Copies of grand jury material will not be mailed to DCIS Headquarters.

28.9.e. **Special Handling.** All confidential informant-related information requires special handling and restricted dissemination in accordance with SAM Chapter 7, “Confidential Informants.” Any reference to a confidential informant in a Form 1 or investigative report should in no way identify the confidential informant, other than by their assigned confidential informant number.

28.9.f. **Sensitive or Classified Investigations.** If classified, the CIR, Case Summary–Update, ROI, Case–Termination, or IR will not be uploaded into CRIMS. Contact the Program Director, National Security Program, for further guidance regarding the preparation, marking, storage, accountability, reproduction, transmission, transportation, or disposal of any classified documents. Also see SAM Chapter 2 for guidance on sensitive or classified investigations.

28.10. Use of the Form 1 for Case Initiations

28.10.a. **Reporting Deadlines.** The CIR Forms 1 will be drafted and submitted for supervisory approval **within 15 calendar days** after receipt of information sufficient to initiate an investigation and uploaded into the CRIMS VCF within **30 calendar days**. Any delays in opening an investigation, such as unavailability of a major witness or awaiting coordination with an MCIO should be explained in the CIR. The CIR will list all participating law enforcement agencies. The results of any related MCIO decision must be reported, to include the date, name, and title of the individual with whom coordination was made. A search of CRIMS will be conducted by the OPR to determine if other DCIS offices have any ongoing investigations involving the suspects. Attachments N – R are examples of CIR Forms 1.

28.10.b. Joint Investigative Agencies and Coordination. To ensure the most effective use of investigative resources, contact any MCIO, other agency, and DCIS office affected by the investigation. For example, the San Francisco RA would be required to coordinate with the New York RA on an investigation of a corporation in the New York RA AOR. Agencies or offices may alternate preparation of reports that function as Forms 1, provided the participating agencies do not document the same investigative activity. The fact that an investigation is being conducted with another investigative organization will also be reflected in CRIMS by the OPR. Only one agency should prepare the final ROI, with input, as appropriate, from participating agencies.

28.10.c. Narrative. The narrative of the CIR Form 1 will report the basis for the investigation, indicate the source of the information or allegation, and state the reason for the initiation of the investigation. The CIR must contain the date the information was received. The narrative should not exceed three pages in length, unless special circumstances are warranted. Sufficient facts must be reported in the narrative to allow it to stand on its own merit; details will not merely be incorporated by reference to an attachment, such as DCAA referral. The allegation should be fully addressed in the text. The narrative of the CIR Form 1 will address the basic who, what, when, where, why, and how questions. The CIR should also clearly state the focus and objective of the investigation. The following are examples of the types of details that should be included in the narrative of a CIR.

(b)(7)(E)

(b)(7)(E)

28.10.d. **Dissemination.** CIRs will be disseminated at the local level to the appropriate DoD legal counsels and other DoD agencies, as deemed appropriate by the SAC/ASAC/RAC. If a military service is affected, a copy of the CIR will generally be forwarded to the local MCIO. If allegations are received that may be of interest to other Federal agencies (such as the IRS or the FBI), the OPR should coordinate with those agencies as soon as practical, to include providing them a copy of the CIR, if the SAC/ASAC/RAC deems appropriate. If dissemination of the CIR Form 1 is to be restricted, it will be accomplished in accordance with paragraph 28.9.c.

28.10.e. **Case Initiation/Closed.** In certain instances a Case Initiation/Closed may be used in lieu of the initiation of a regular investigation. A Case Initiation/Closed is used to document investigative work such as an arrest, recovery, or seizure. It will only be used in investigations that are completed **within 15 calendar days**, to include prosecutorial, administrative, or other adjudicative activity. The Case Initiation/Closed will also serve as the closing ROI and will be entered into CRIMS as such.

28.10.f. **Case Reopening.** On occasion, a case must be reopened after it is closed. The SAC or ASAC will be the approval authority for all case reopenings. A Form 1 will be used to reopen an investigation and will be sent as an e-mail attachment to Internal Operations through the CRIMS PMO general mailbox at INV-CRIMS-Help@dodig.mil **within 15 calendar days** of the date it is determined the investigation should be reopened. The CRIMS Admin Team will be responsible for uploading the case reopening Form 1 to the VCF. The Form 1 must provide a sufficient explanation of why the investigation was reopened, such as fugitive located or delayed administrative settlement or action. See Attachment S for an example of a Request for Case Reopening Form 1.

28.11. Use of the Form 1 for Investigative Projects

28.11.a. **General.** The DCIS Form 1 is used to initiate investigative projects (b)(7)(E)

(b)(7)(E)

Attachment T is a sample of a CIR for an investigative project.

28.11.a.(1). The following are examples of appropriate use of investigative projects.

(b)(7)(E)

(b)(7)(E)

28.12. Use of the Form 1 for Operational Purposes

28.12.a. **General.** The Form 1 is the basic reporting document used to record all actions in an investigation. These investigative actions include traditional operational matters such as interviews and searches, as well as supporting matters such as a request for a polygraph examination. The Form 1 will be used to report the results of investigative actions and to synopsise or describe the individual attachments that concern the activity reported, such as photocopies of evidentiary documents, review of records, and review of contract files. All Forms 1 documenting routine operational activities must be drafted and submitted for supervisory approval **within 15 calendar days** after the action has been accomplished. All Forms 1 will be retained in the official file after approval. Forms 1 and related attachments will be uploaded into the CRIMS VCF **within 30 calendar days** of the date of the investigative activity. In a joint investigation with another agency, copies of the joint agency's reports (such as FBI Forms 302) will be retained in the official case file. Forms 1 may also be used as exhibits to ROIs (see paragraph 28.18.b.). Reports received from joint investigative agencies and incorporated into the official case file should be uploaded into the VCF unless the authoring agency's policy expressly prohibits this. Attachment U is a sample Form 1.

28.12.b. **Form 1 Preparation.** The narrative portion of the Form 1 will be written in the third person and will detail the activity that has occurred. The document will reflect the names of any agents and other participants present at the reported activity. Personal opinions, recommendations, or conclusions of the agent will not be reported in a Form 1.

28.12.b.(1). Forms 1 must be written so the reader will understand why it was written and how it relates to the investigation. The document should address the basic who, what, when, where, why, and how questions. The Form 1 should indicate where the interview or activity took place, unless that information would tend to compromise a confidential informant. For example, a witness interview should include name, title, and relationship to the investigation, and a records review should describe the records.

28.12.b.(2). The use of "Agent's Note" in the text of the Form 1 is restricted to reporting factual, relevant, and substantive observations. When used, the agent's note should be in the main body of the report and preceded by the caption "**AGENT'S NOTE:**" which will be

in upper case letters, in bold, underlined, and aligned to the left margin. Agent's notes may be used, for example, to point out apparent contradictions between the statement of a witness and actual conditions or events. **Agent's notes should be used sparingly.**

28.12.b.(3). Regardless of whether the person interviewed is a suspect, person of interest, witness, or victim, an effort must be made to obtain their PII (such as date and place of birth and SSN), residence address and telephone number, and work address and telephone number. Any PII collected will be documented in the case notes. The data will be entered in CRIMS and not reported in the associated Forms 1. This information could save significant time in locating a witness at a later date. However, an exception to this is, PII will be included in closing ROIs in the "Identity of Suspects" section.

28.12.c. **Reporting Multiple Activities.** Generally, the Form 1 will not be used to report multiple investigative activities. For example, a single Form 1 may not be used to report a records review, an interview, and a search all conducted on the same day. Multiple interviews of the same person will not be reported on the same Form 1, unless the interviews occurred on the same day and concerned the same investigation. A Form 1 with multiple interviews is suitable for reporting unproductive interviews, such as the interview of four individuals in an unsuccessful attempt to locate a neighbor.

28.12.d. **Form 1 Distribution.** If it is necessary to distribute a copy of a Form 1 or another investigative report outside DCIS, such as in a joint investigation or suspension/debarment coordination, approval must be obtained from the applicable RAC prior to any such dissemination. Recipients will be listed in the distribution section of the Form 1. Dissemination of an outside agency report is prohibited without permission from that agency.

28.13. Use of the Form 1 for Lead Requests

28.13.a. **General.** Lead Requests (also known as Requests for Assistance) are used to request investigative assistance between DCIS offices or MCIOs. Lead responses are completed by the assisting DCIS office upon completion of the Lead Request. Lead Requests should contain sufficient information regarding the assistance needed of the MCIO or DCIS office completing the request. The Lead Request Form 1 will contain the abbreviated suspect titling and all appropriate distribution codes. The original Lead Request Form 1 will be retained in the OPR's official case file.

28.13.a.(1). **Policy.** Policy regarding Lead Requests between Defense Criminal Investigative Organizations (DCIOs) shall conform to the spirit and letter of the Memorandum of Agreement (MOA) between DCIS and the MCIOs signed on November 14, 1997, effective December 14, 1997, (a copy of the MOA is appended as Attachment V).

28.13.a.(2). Lead Requests Between DCIS Offices

28.13.a.(2).(a). If assistance is needed from another DCIS office, prior coordination (telephonically or e-mail) should be made with the RAC of the assisting office to ascertain if the assisting office can complete the lead request. Lead requests from one DCIS

office to another DCIS office will be prepared on the Lead Request Form 1 and can be sent via e-mail to the office where the lead will be accomplished. The Lead Request Form 1 will contain the abbreviated suspect titling and all appropriate distribution codes. The original Lead Request Form 1 will be retained in the OPR's official case file. Attachment W is an example of a Lead Request Form 1 between DCIS offices.

28.13.a.(2).(b). Responses to lead requests between DCIS offices will be prepared on the Lead Response Form 1. Responses must be completed **within 15 calendar days** after Lead Requests are received. The assisting office will notify the OPR by telephone or e-mail if this deadline cannot be met. The Lead Response Form 1 will contain all appropriate distribution codes and may be forwarded to the OPR as an e-mail attachment for retention in the official case file. The response will reference the lead request in the first paragraph; the actual Lead Request Form 1 will not be appended to the Lead Response Form 1. All agent's notes should be returned in an envelope to the OPR with the lead response. See SAM Chapter 4, "Interviews and Interrogations."

28.13.a.(3). Lead Requests Between DCIOs

28.13.a.(3).(a). A Lead Request may be made by the DCIS OPR to an MCIO in writing, electronically (such as facsimile transmission or e-mail), or by telephone. If the MCIO receiving the request agrees to assist, the OPR must prepare a Lead Request Form 1 and include the MCIO in the distribution.

28.13.a.(3).(b). The Lead Request Form 1 will contain the OPR's CN, complete identification of the suspects of the investigation, a summary of the matter under investigation, a clear statement of the assistance requested, and the name and telephone number of the case agent responsible for the matter under investigation. Copies of supporting documents and exhibits will be provided with the Lead Request when applicable. The original Lead Request Form 1 will be retained in the OPR's official case file. Attachment X is an example of a Lead Request Form 1 to an MCIO.

28.13.a.(3).(c). If the OPR determines the required information can be obtained by means other than the Lead Request, then those means should be pursued whenever feasible. Direct correspondence with governmental offices/agencies or commercial businesses is encouraged to conserve investigative resources and expedite completion of requests for information. For example, official letterhead correspondence should be directed to state or county offices to obtain copies of ordinary business records such as birth certificates, business licenses, and state corporation records. The SAC will sign all official correspondence. The SAC may delegate the signature authority to the ASAC or the RAC.

28.13.a.(3).(d). Case agents and supervisors are responsible for ensuring Lead Requests seeking only meaningful information are dispatched. If a Lead Request is declined, a Form 1 must be prepared to document the Lead Request and the MCIO's declination to assist.

28.13.a.(3).(e). After a DCIS office has agreed to a Lead Request and has received a formal written Lead Request from the requesting MCIO or another agency, the DCIS office conducting the lead will prepare an External Lead Response IR with (b)(7)(E) to document that action. Responses must be completed **within 15 calendar days** after the formal written Lead Request is received. The DCIS office will notify the requesting MCIO by telephone or e-mail if the response cannot be accomplished **within 15 calendar days**. The External Lead Response IR will be sent directly to the requesting MCIO, with a copy to the responding DCIS office's associated FO if the office is an RA or POD. The External Lead Response IR will reference the Lead Request in the first paragraph with a copy of the actual Lead Request appended as an attachment. The External Lead Response IR will contain all appropriate distribution codes, including any other DCIS offices involved and the requesting MCIO.

28.14. Use of the Form 1 for Requests for Other Types of Operational Support

28.14.a. The Form 1 will function as the document to request other types of support, such as polygraph examination, computer forensics/analysis, or technical services. All such Forms 1 will be forwarded to the appropriate DCIS Headquarters program. For guidance on how to prepare requests for these types of support see SAM Chapter 12, "Technical Services Program;" SAM Chapter 40, "Cyber Crimes Program;" and SAM Chapter 57, "Polygraph Examinations."

28.15. Use of the Form 1 for Case Summary–Updates

28.15.a. **General.** The CIR is considered the initial Case Summary. The first update will contain a summary of the events that occurred and any changes (such as estimated loss to the DoD, joint agency participation, or DOJ case acceptance) **within 90 calendar days** of the date of the CIR. The initial update paragraph will be placed below the initial CIR narrative and will reflect the date of the Case Summary–Update reporting period (for example, March 1, 2010, Update). Every 90 days thereafter, a summary of the activity that occurred since the last update will be appended to the Case Summary–Update. All investigative activity and results reported in Case Summary–Updates must be appropriately documented in the official case file. However, Case Summary–Updates for investigations placed in "suspense" status are required twice a year. For the example above, the update will be completed and placed in the official case file **within a timely manner** of the date the report was approved by the supervisor. The Case Summary–Update can be conformed to a schedule for each agent; however, the first Case Summary–Update will not be longer than **90 calendar days** from the case initiation date. Exceptions can be made if supervisors cycle case summaries on new summary dates to conform to a consistent schedule. A statement should be entered to reflect the adjustment of case summary dates, especially when there is a delay.

28.15.b. The online Case Summary–Update is a significant source of information regarding an ongoing investigation. The Case Summary–Update must contain sufficient detail to explain the allegations, investigative activity, relevant issues, and significant accomplishments to date. The author, distribution, and approval blocks will be placed at the bottom of the last page of the Form 1. If any of the categories or criteria are met or change after the investigation was initiated for SIC factors, referral sources, estimated loss to the Government or joint investigative

agencies, the new information will be reflected on the Case Summary–Update in the applicable sections and entered into CRIMS accordingly. Attachment Y is an example of a Case Summary–Update.

28.15.c. **UCO Cases.** The Case Summary–Update for an UCO should include the total number of suspects identified to date, the total number of spinoff cases and IRs generated from the UCO, the case title, and UID. Distribution for Case Summary–Updates relating to UCOs will be restricted. See SAM Chapter 9 for further guidance on the reporting requirements for UCOs.

28.15.d. **Distribution.** Case Summary–Update and other DCIS reports may be distributed to the DCIOs, other law enforcement, and other DoD agencies at the discretion of the RAC.

28.16. Use of the Form 1 for Reporting Significant Incidents

28.16.a. **Significant Incident Report (SIR).** Generally, a SIR Form 1 will be prepared and approved by the supervisor **within 15 calendar days** following the reportable significant event and placed in the official case file. If the supporting documentation for the significant incident is not available within the 15 calendar day timeframe, the SIR Form 1 will not be approved until such documentation is available. The case agent will make the appropriate CRIMS entries for any investigation for significant events or incidents. If any case with DCIS involves a recovery of \$500,000 or more, the supervisor cannot validate the SIR and supporting documentation in CRIMS. Validation of recoveries of \$500,000 or more must be reviewed and approved by Internal Operations. Further guidance and examples of significant events and supporting documentation can be found in SAM Chapter 50.

28.16.a.(1). SIR Forms 1 must include a brief synopsis of the case, to include the basis of the investigation. See below for examples of significant incidents. All Forms 1 reporting any of the events listed below will no longer contain the special report banner titled “**SIGNIFICANT INCIDENT REPORT.**” Attachments Z, AA, BB, CC, and DD are examples of SIR Forms 1.

(b)(7)(E)

(b)(7)(E)

28.17. Use of the Form 1 for Reports of Investigation

28.17.a. **General.** The ROI is used to present investigative findings for prosecutorial, civil, or administrative actions. The ROI may be disseminated outside DCIS to those parties having a need to know. See paragraph 28.9. for guidance on dissemination of DCIS reports. The ROI will be prepared on the Form 1. Generally, only one ROI will be submitted in an investigation, although certain situations require interim ROIs (for instance, if requested by a prosecutor). All investigations require an ROI, except when a Case Initiation/Closed or Case Termination Form 1 is used. If any individual listed in the title of the investigation was not interviewed during the investigation, an explanation for not conducting the interview must be provided in the ROI. An ROI can be used to terminate an investigation by reflecting the appropriate case disposition code after the CN.

28.17.a.(1). All ROIs must include a statement on whether fraud vulnerabilities were identified during the course of the investigation. If applicable, include the date the notice of fraud vulnerability notice was submitted to DCIS Headquarters. All ROIs must include a statement on whether administrative action was taken during the course of the investigation, to include, but not limited to, suspension or debarment, and suspension or termination of security clearances. See SAM Chapter 25, “Coordination of Remedies,” for further guidance on suspension and debarment coordination.

28.17.a.(1).(a). If the investigation involves a defective product, non-conforming product, counterfeit product, or product substitution in which a serious hazard to health, safety, or operational readiness is identified, the ROI must include a statement on whether a Notice of Suspected Defective Product Memorandum or GIDEP notification was issued. See SAM Chapter 25 for further guidance on the preparation of Suspected Defective Product Notifications.

28.17.a.(1).(b). SACs may delegate approval authority for ROIs to ASACs, RACs, or Program Directors.

28.17.b. Reports of Investigation. Generally, there are two types of ROI formats: Prosecutorial and Condensed. NOTE: ROIs will not contain a “Referral Source(s) section on the cover page. The referral source(s) should be reflected in the “Background” or “Narrative” section of the applicable ROI format.

28.17.b.(1). Prosecutorial ROI Preparation. The ROI prepared for prosecutorial purposes is a very detailed presentation of investigative findings. This type of report is normally prepared only at the request of the prosecutor prior to the conclusion of an investigation. In preparing ROIs intended for criminal prosecution or civil action, sections will be labeled numerically, beginning with the “SYNOPSIS” section. Attachment EE is an example of a Prosecutorial ROI.

28.17.b.(1).(a). Cover Page. The cover page contains the CN and date of the report, as well as the complete name of all suspects of the investigation. Each person will be listed by complete name, and each business or non-personal suspect will be listed by name and location. The lower left corner will reflect the distribution of the ROI. Acronyms may be used in the distribution section if the acronym is commonly used and known, thereby allowing the reader to readily identify the recipient.

28.17.b.(1).(b). Table of Contents. Self-explanatory.

28.17.b.(1).(c). Synopsis. All ROIs prepared for prosecutorial purposes will contain a synopsis. This section will be a concise summary of the allegations and results of the investigation and will establish the basic elements of proof for offenses documented by the investigation. It will include the dollar value of a loss or recovery if such occurred.

28.17.b.(1).(d). Statutes. All ROIs prepared for prosecutorial purposes will contain a statutes section. This section will cite the specific violations of the United States Code or other Federal or state violations.

28.17.b.(1).(e). Background. This section will present a factual account of the basis for the investigation and any action that transpired prior to initiation of the investigation.

28.17.b.(1).(f). Special Program Information. This is an optional section that describes a DoD program, procedure, or regulation crucial to understanding the offense. For

example, “Progress Payments” and “Foreign Military Sales” would be considered special programs requiring some explanation. This information may be incorporated into the narrative.

28.17.b.(1).(g). Narrative. This section will present the results of the investigation, with emphasis on offenses rather than steps taken in developing the investigation. The narrative will present sufficient information to clearly describe the manner in which criminal and civil violations occurred and what evidence was collected in support of the findings. The ROI will not contain conclusions, recommendations, or opinions and will be structured as follows.

28.17.b.(1).(g).1. The narrative will be presented in continuously numbered paragraphs under descriptive headings in chronological order. The content of Forms 1 may be summarized in the narrative and relevant Forms 1 may be appended as exhibits. Another method of report writing is to present the evidence in a narrative fashion with the emphasis being on the evidence itself, rather than on individual interviews. The writing style and method of report writing of the narrative is left to the discretion of the writer and reviewing supervisor. It will be governed by the investigative methodology, the complexity of the investigation, and, in some cases, the desires of the prosecutor.

28.17.b.(1).(g).2. Any exhibits, such as sworn statements, Forms 1, photographs, and other documentary materials appended to the ROI will be identified when referred to in the narrative and will be listed sequentially in the Exhibits section.

28.17.b.(1).(g).3. Observations of the investigator, such as contradictions between witness statements and actual events, or the suspect’s condition and appearance during the interview may be appropriate, provided this information is plainly set off from the general text of the ROI and is clearly identified as an **AGENT’S NOTE**.

28.17.b.(1).(g).4. The fact that a polygraph examination has been administered to an individual on a particular date should be reflected in the narrative. However, relevant test questions and answers and the technical results (conclusions) should not be listed in the ROI. It is recommended that a polygraph examination Form 1 be included as an exhibit, with limited distribution to the appropriate officials responsible for personnel security, intelligence, counterintelligence, law enforcement, and the administration of justice, in accordance with DoD Directive 5210.48, “Polygraph and Credibility Assessment Program,” Change 2, November 15, 2013. Polygraph examination refusals will not be addressed in the ROI.

28.17.b.(1).(h). Evidence (Subjects/Documents/Witnesses). This section will be used to fully identify all witnesses who can provide testimony and to describe in detail the relevance and significance of evidence collected. The testimony each witness can provide will be briefly described, along with a description of the evidence the witness can introduce at a trial, if necessary. Forms 1 reflecting complete interviews should be attached as exhibits. If the evidence was submitted for laboratory analysis, the results will be summarized and the report appended as an exhibit. Similar to preparation of the narrative, the style of presenting witnesses/suspects and evidence depends on the writer/supervisor and the information to be presented.

28.17.b.(1).(i). Status of Investigation. This section will report either the results of prosecution or the fact that prosecution is anticipated. This section will also be used to place a case into suspense status, to report prosecutorial declinations, or to close an investigation.

28.17.b.(1).(j). Prosecutorial Considerations. This section, if required, may be used to set forth special prosecutorial considerations, such as immunity provided to a witness.

28.17.b.(1).(k). Identity of Suspects. This section reports the identifying data for all suspects in the investigation. At a minimum, this page will include name, alias, SSN, date and place of birth, race, sex, last known residence, last known occupation, and driver's license number and issuing state.

28.17.b.(1).(l). Exhibits. This section will identify and describe each exhibit as it is referred to sequentially in the narrative of the ROI. Exhibits will be numbered only.

28.17.b.(2). **Condensed ROI Preparation**. Condensed ROIs are most commonly used for closing investigations. The condensed ROI can be prepared for investigations that have been resolved criminally and civilly, as well as for matters that will not be prosecuted or pursued civilly. The ROI for an investigation closed as unfounded, declined for prosecution, or resulting in administrative remedies/personnel actions may be reported in a condensed format. The ROI will have a "Cover Page," a "Narrative," and "Identity of Suspect(s)" sections, and an "Exhibit(s)" section (if appropriate). Typically, condensed ROIs will not contain an "Exhibits" section, unless the investigation is being referred to an outside agency. All Forms 1 prepared in the investigation should be filed in the official case file prior to the final ROI being placed in the official case file. Exceptions will be made if supplemental information is received after an investigation has been closed. Any supplemental information received should be documented in a Form 1 and filed after the ROI in the closed case file. Although written in a condensed format, sufficient information will be reported to document all investigative effort, to include dates of interviews and significant activity. If any individual listed as a suspect of the investigation was not interviewed during the investigation, an explanation for not conducting the interview must be provided in the final ROI. The condensed ROI may also be used when a detailed ROI was not required and all prosecutorial action has been completed. This usually occurs when a prosecutor has been continually involved since the early phases of an investigation and does not require a prosecutorial ROI prior to prosecution. In this circumstance, a condensed ROI may be submitted at the end of the investigation. A condensed ROI shall be completed and entered in CRIMS **within 45 calendar days** after the last investigative effort or declination for prosecution, whichever is the most recent action. Attachment FF is an example of a Condensed ROI.

28.17.c. **Supplemental ROIs**. On occasion, an investigation completed by DCIS may be reopened by the same OPR for further investigation. In those instances, a Supplemental ROI will be prepared, using one of the preceding formats, as appropriate, when the additional investigation is completed. The Supplemental ROI should document the reason the investigation

was reopened and include all investigative activity following the reopening. The Supplemental ROI will supplement, not replace, the original ROI in the official case file and the online system, and will be e-mailed to Internal Operations **within 45 calendar days**.

28.17.d. Use of the ROI to Suspend an Investigation. When all investigative efforts are complete, and a delay is anticipated in prosecution, or civil or administrative action, an ROI will be submitted reflecting a “suspense” status. A brief comment that the case is in suspense will be contained in the “narrative” section of the ROI. If an ROI was submitted before placing the case into suspense, a supplemental Form 1 will be submitted reflecting the change to a suspense status in the narrative paragraph of the report, and the case disposition/status will be updated in CRIMS accordingly. Case Summary–Updates for investigations placed in “suspense” status are required twice a year. The first case summary update for this type of investigation will be completed within six months of the date the investigation was placed in suspense and every six months thereafter until the investigation is officially closed. When all remaining activity has occurred or it is determined the investigation should be officially closed, a supplemental Form 1 will be submitted to document any remaining activity and the reason for closing the investigation. The supplemental Form 1 will also include the applicable case disposition code after the CN on the final report and retained in the official case file. The case disposition code/status will also be updated in CRIMS to officially close the investigation.

28.17.e. Use of the Form 1 for Case Terminations. Generally, an ROI is prepared to close or cancel a DCIS investigation. However, a Case Termination Form 1 can be used to cancel or close an investigation if a DCIS or joint agency ROI was previously submitted or if the investigation has not been open more than 90 days and there has been limited investigative activity conducted. If a case is canceled, the Case Termination Form 1 or ROI must explain why the case has been canceled (such as an objective determination that the potential for successful resolution of the investigation does not exist or if directed by the associated SAC or DCIS Headquarters). (b)(7)(E) When a Case Termination Form 1 is used to close an investigation, the appropriate case disposition should be used to address the reason the case is being closed. The complete names and locations of all suspects of the investigation will be listed similar to the ROI cover page format.

28.17.e.(1). Case Termination Form 1 for Joint Investigations. Only one agency should prepare the final ROI, with input, as appropriate, from participating agencies. Similar to ROIs, the Case Termination Form 1 will address all DoD-related issues if they are not included in the outside agency’s ROI, such as discovery of fraud vulnerabilities and results of coordination of remedies. Attachments to such ROIs may include Forms 1 and investigative reports prepared by other agencies. The OPR will prepare a Form 1 cover page for the joint agency ROI. The Case Termination Form 1 will be posted as the online ROI. This Form 1 will briefly explain the background and significance of the other agency’s ROI and contain the statement: “A copy of the joint agency ROI has been received and is retained in the official file.” Attachment JJ is a sample Case Termination Form 1 where the joint agency prepared the final ROI.

28.17.e.(2). **Case Termination Form 1 When No ROI Is Submitted.** The Case Termination Form 1 will be submitted to cancel an investigation when no ROI has been previously submitted. The use of this Case Termination Form 1 will only be utilized when limited investigative activity has been conducted and the investigation has not been open longer than 90 days. However, SAC approval must be obtained to cancel an investigation without an ROI. **The use of this method to close an investigation should be used sparingly.** Attachment KK is a sample Case Termination Form 1 where no ROI was submitted.

28.18. Use of the Form 1 for Information Reports

28.18.a. **General.** An Information Report Form 1 will be prepared if an allegation is received where, following a preliminary review/inquiry, it is determined not to warrant the initiation of an investigation by the receiving office. A preliminary review/inquiry is defined as the minimum effort necessary to determine if the allegation merits a DCIS investigation. The results of any related investigative activity or substantive effort (for example, the results of interviews or record reviews) should be reported in the IR Form 1. Additionally, an IR will not be used to report any of the following investigative actions: an arrest of any individual; an allowable seizure of property, funds, or fruits and instrumentalities of an offense; or a referral for an adjudicative determination (criminal, civil, or administrative). In the event that any of these actions occur, a regular investigation or a Case Initiation/Closed must be opened and actions reported therein.

28.18.b. **Preparation of the Information Report.** Preparation of the IR Form 1 and procedures for distribution and approval are similar to the CIR Form 1. An IR must be prepared **within 15 calendar days** after receipt of information sufficient to document the matter in an IR. The office intending to issue an IR must search CRIMS to determine if prior information on the suspect exists and if other DCIS offices have an interest in the information. The search results must be reflected in the IR.

28.18.c. Types of Information Reports

(b)(7)(E)

(b)(7)(E)

28.18.c.(4). Receipt of Supplemental Information (Information Report).

When a DCIS office receives supplemental information after an Information Report (b)(7)(E) is prepared, the information will be assessed in conjunction with the original IR to determine if the initiation of an investigation is warranted. If no investigation is warranted, a supplemental Form 1 will be prepared to document the receipt of this type of information and retained in the hard copy case file of the original IR. Coordination must also be made with Internal Operations to upload the supplemental Form 1 into the CRIMS VCF associated with the original IR. Attachment OO is a sample Supplemental Form 1.

28.19. DoD OIG Audit Coordination Memorandum

28.19.a. General. Effective coordination between DCIS and ODIG-AUD is essential to carrying out the DoD IG's mission as well as the timely reporting of systemic weaknesses that may impact DoD. The Audit Coordination Memorandum (ACM) will be used to request ODIG-AUD support on investigations and to report the discovery of fraud vulnerabilities potentially impacting DoD entities or its programs. Attachment PP is a sample of an ACM.

28.19.a.(1). Requests for DoD OIG Audit Assistance. When ODIG-AUD support is required on an investigation, the case agent will prepare an ACM, upon concurrence of the SAC (or designee), to be forwarded to the appropriate Desk Officer/Program Manager for review via e-mail to DCIS Headquarters at INV-003@dodig.mil. Upon approval of the appropriate AIGI (or designee), the request will be forwarded to the Principal Assistant Inspector General for Auditing (PAIG-AUD) for review and assignment of the appropriate audit support. All requests should include a description of the support requested to allow the PAIG-AUD to fully assess the amount of time and audit resources required to support the investigation. A copy of the signed ACM will be returned to the OPR to be filed in the official case file, and CRIMS should be updated to reflect the request for technical assistance.

28.19.a.(2). Fraud Vulnerability Reporting.

(b)(7)(E)

(b)(7)(E)

Fraud vulnerability is a condition in which the internal controls or compliance with those controls does not provide a reasonable assurance that systems within DoD are adequately protected against fraud, waste, or abuse. Fraud vulnerability is generally systemic and is not an isolated incident. Fraud vulnerability may be caused by a lack

of appropriate controls or inadequate compliance with existing controls. For example, a fraud vulnerability can be a lack of internal controls that allows a violation, such as a willful criminal violation of law to occur or go undetected.

28.19.a.(2).(a). When a fraud vulnerability is identified, the case agent will prepare an ACM, upon concurrence of the SAC (or designee), to be forwarded to the appropriate Desk Officer/Program Manager for review via e-mail to DCIS Headquarters at INV-003@dodig.mil. Upon approval of the AIGI-INV (or designee), the memorandum will be forwarded to the PAIG-AUD for information and any action deemed appropriate. A copy of the signed memorandum will be returned to the OPR to be filed in the official case file. This type of ACM should be uploaded into CRIMS under the document type “ACM/Fraud Vulnerability Report.”

28.19.a.(2).(b). The OPR should coordinate the reporting of fraud vulnerabilities with all participating agencies, if applicable, and the Assistant U.S. Attorney, if one is assigned, and the appropriate authorities within the affected DoD Components. Fraud vulnerability notices are generally issued following the completion of judicial proceedings or prior to closing the case. However, coordination with the appropriate authorities within the affected DoD Components and the issuance of fraud vulnerability notices can be done at any stage in the investigation if the issuance of the notice does not have an adverse impact on operational security of the investigation.

28.20. Coordination of Remedies Reporting Requirements

28.20.a. **General.** In accordance with DoD Instruction 7050.05, “Coordination of Remedies for Fraud and Corruption Related to Procurement Activities,” May 12, 2014, the DoD IG and other DoD components are required to monitor, from inception, all significant investigations of fraud or corruption related to procurement activities affecting their organizations. The monitoring must ensure all possible criminal, civil, contractual, and administrative remedies are identified to applicable procurement and command officials and DOJ officials, as appropriate, and that appropriate remedies are pursued expeditiously. This process must include coordination with all other affected DoD Components.

28.20.a.(1). **Suspected Defective Product Notification.** In accordance with DoD Instruction 7050.05, DCIS Headquarters is required to (1) expeditiously notify the Centralized Organization of the initiation of all investigations involving allegations of non-conforming products, defective products, product substitution, or counterfeit materiel, (2) continue to provide to the centralized organizations any information developed during the course of the investigation that indicates a suspect product has been, or might be, provided to the DoD, and (3) require that any request for testing of the suspect product is provided to the centralized organizations. NOTE: The FO SAC (or designee) should not delay making immediate notification to the appropriate Centralized Organizations if any investigation involves suspect products with potential safety and/or readiness issues. However, the preparation of the Suspected Defective Product Notification should subsequently be submitted to DCIS Headquarters for formal dissemination.

28.20.a.(2). **Suspension and Debarment Coordination.** In accordance with DoD Instruction 7050.05, DCIS is required to notify Centralized Organizations of the initiation of all significant investigations of fraud or corruption related to procurement activities affecting its organization. The notification will allow the affected DoD components to determine and implement appropriate contractual and administrative remedies to recover funds lost through fraud or corruption and to ensure the integrity of DoD programs and operations. RACs will prepare these notifications and send them to the Coordination of Remedies Program Manager for the appropriate dissemination.

28.20.a.(3). **Security Clearance Coordination.** In accordance with DoD Instruction 7050.05, DCIS is required to notify the appropriate adjudication facility of any findings of procurement-related fraud or corruption perpetrated by cleared personnel and facilities for an assessment and determination of continuing eligibility for a security clearance. RACs will prepare these notifications and disseminate them to the appropriate adjudication facility.

28.20.b. See SAM Chapter 25 and DoD Instruction 7050.05 for further guidance on the reporting requirements referenced above. Contact the Coordination of Remedies Program Manager for the latest versions of the coordination of remedies notices referenced above.

28.21. **Other Required Reporting**

28.21.a. **Reporting of Conflict of Interest Violations to OGE.** The Director of the U.S. Office of Government Ethics (OGE), in accordance with 5 U.S.C. App. § 402(e)(2), has promulgated regulations (5 C.F.R. § 2638.603) requiring agencies to concurrently notify OGE when matters involving a violation of 18 U.S.C. §§ 203, 205, 207, 208, or 209 (conflict of interest statutes) are referred to DOJ and the disposition of these referrals, unless such notification would otherwise be prohibited by law. To accomplish this notification requirement, agencies are required to complete the OGE Form 202, Notification of Conflict of Interest (Attachment QQ). Further, the DoD Standards of Conduct Office (SOCO) is charged with ensuring DoD agencies administer and maintain a comprehensive ethics program in accordance with DoD Directive 5500.07, “Standards of Conduct,” November 29, 2007, and DoD 5500.07-R, “The Joint Ethics Regulation (JER),” November 17, 2011.

28.21.a.(1). **Initial Notification.** DCIS RACs will ensure conflict of interest violations referred to DOJ are reported on OGE Forms 202 and sent to the appropriate desk officer/program manager for review via e-mail to DCIS Headquarters at INV-003@dodig.mil. The desk officer/program manager will send the OGE Form 202 to OGE with a courtesy copy to the OPR and SOCO. The OPR will maintain a copy of the OGE Form 202 in the hard copy case file and upload a copy into the CRIMS VCF under the document type “OGE Form 202.”

28.21.a.(2). **Notification of Disposition.** Agencies are also required to notify OGE’s Director of each referral’s disposition, including any disciplinary or corrective action taken by the department or agency, via the OGE Form 202. Upon the conclusion of these investigations, RACs will update the “Disposition of Referral” section of the OGE Form 202, as appropriate, and send the form to the appropriate desk officer/program manager for review via

e-mail to DCIS Headquarters at INV-003@dodig.mil. The desk officer/program manager will send the updated OGE Form 202 to OGE with a courtesy copy to the OPR and SOCO. The OPR will maintain a copy of the updated OGE Form 202 in the hard copy case file and upload a copy into the CRIMS VCF under the document type “OGE Form 202.”

28.22. Case Review Requirements

28.22.a. **General.** RACs are required to conduct investigative case reviews to ensure investigations (not including investigative projects) are being thoroughly conducted and reports are being written accurately, clearly, and concisely. Special agents must ensure the case file includes documentation of all reportable investigative activity. Supervisors are responsible for verifying that the critical case data in CRIMS is accurate and up-to-date. Supervisors will review investigative case files twice each fiscal year (no later than March 31 and September 30) to ensure each investigation is progressing in an efficient, effective, thorough, objective, and legal manner. These case reviews will be documented on a DCIS Form 5, Case Review Record, and Form 5A, Case Review Continuation Page. NOTE: These investigative case reviews are required for cases placed in a “suspense” status. See SAM Ch. 50 for guidance on how to capture the completion of case reviews in CRIMS.

28.22.a.(1). **Case Review Record.** The supervisor will complete the Form 5 and maintain this document separately from the official case file. The Forms 5 and 5A will only be incorporated into the hard copy case file along with the case notes at the conclusion of the investigation. Neither form will be uploaded into the CRIMS VCF. Attachment RR is a sample DCIS Form 5 and Attachment SS is a sample DCIS Form 5A. See SAM Chapter 42 for further guidance on case file management.

28.23. Case Closing Actions

28.23.a. **Case Notes.** Courts have ruled that agents have a legal obligation to maintain original notes; the agent may be required to produce the notes during legal proceedings. E-mail communications have been characterized as “electronic records” for purposes of discovery and the Freedom of Information Act. Investigative notes include, but are not limited to, notes used to prepare a Form 1, substantive notes taken by the agent, memoranda of telephone calls, telephone interviews, investigative plans, thought processes, agent’s work product, and notes that could have evidentiary value. It is recommended that administrative notes, such as Case Review Records and those notes not related to the substantive investigation also be maintained separately until the investigation is closed. See Attachment TT for DOJ guidance on discovery practices.

28.23.a.(1). **Agent’s Case Notes.** Case notes will be maintained, by the agent, separate from the official case file until the case is closed. On completion of the investigation, the investigative notes will be placed in the official case file. All notes must clearly identify the agent, investigation, activity date, and investigative activity, if applicable. The agent’s notes will be placed separately in a sealed envelope labeled with the CN, case title, and agent’s or supervisor’s name.

28.23.a.(2). **Supervisory Notes.** The supervisor will maintain the Form 5 separately from the official case file until the case is closed. The Form 5 will be placed in a sealed envelope labeled with the CN, case title, and supervisor's name. On completion of the investigation, the envelope containing the Form 5 will be placed in the official case file. The Form 5 is not to be uploaded into CRIMS.

28.23.a.(3). **Reports from Certain External Investigative Databases.** Reports generated from certain investigative databases should be destroyed at the conclusion of the investigation, such as NCIC, FinCen, SAR, and TECS. See paragraph 28.2.d.(1). for further guidance.

28.23.b. **Official Case File and CRIMS.** A DCIS Form 4, Case Closeout Checklist, will be utilized in conjunction with closing an investigation to ensure the official case file is complete and CRIMS is updated to the fullest extent possible. Furthermore, the Form 4 will be used as a guide to ensure efforts were taken to exhaust all investigative and administrative remedies. At the conclusion of an investigation, the Form 4 will be incorporated into the official case file and placed in the last official case folder (on the right side). The Form 4 will be uploaded into the CRIMS VCF. Attachment UU is a sample Form 4 that identifies actions that are to be taken prior to closing a case. RACs will complete the Form 4 to ensure completion steps are taken, to include, but not limited to, the following steps.

28.23.b.(1). **Evidence.** Ensure all evidence obtained during the investigation is disposed of appropriately. See SAM Chapter 18, "Evidence Custody System," for guidance.

28.23.b.(2). **Search Warrant Material.** Ensure all search warrant material obtained during the investigation is disposed of appropriately. See SAM Chapter 19, "Searches," for guidance.

28.23.b.(3). **DoD Inspector General Subpoenaed Material.** Ensure all records obtained by Inspector General subpoenas, during the investigation, are disposed of appropriately. See SAM Chapter 13, "Inspector General Subpoenas," for guidance.

28.23.b.(4). **Other Subpoenaed Material.** Ensure all grand jury, civil investigative demand, authorized investigative demand, HIPAA, or other subpoenaed material obtained during the investigation is disposed of appropriately.

28.23.b.(5) **Other investigative records too voluminous to include in the official case file.** At the conclusion of the investigation, these hard copy documents and electronic medium should be stored in the OPR and disposed of or retired in accordance with SAM Chapter 42.

ATTACHMENTS

- A. Sample Generic Form 1
- B. Sample Generic Case Initiation Report (CIR) Form 1
- C. Sample Case Initiation Report – Corrected Form 1
- D. Sample Supplemental Information Form 1
- E. Case Category Codes
- F. Case Disposition Codes
- G. Sample Title Change Form 1 (Ex. 1)
- H. Sample Title Change Form 1 (Ex. 2)
- I. Common Use Acronyms & Use of Abbreviations
- J. Suggested Form 1 Report Titles
- K. Special Interest Case (SIC) Factors
- L. Sample Information Report/Referred Form 1 (b)(7)(E)
- M. Sample Referral Sources and Tracking Number Format
- N. Sample Case Initiation Report Form 1 (Ex. 1)
- O. Sample Case Initiation Report Form 1 (Ex. 2)
- P. Sample Case Initiation Report Form 1 (Ex. 3)
- Q. Sample Case Initiation Report Form 1 (Ex. 4)
- R. Sample Case Initiation Report Form 1 (Ex. 5)
- S. Sample Request for Case Reopening Form 1
- T. Sample Project Case Initiation Form 1
- U. Sample Form 1 (Operational Purposes)
- V. Memorandum of Agreement Between the DCIS and MCIOs, dated November 1997

- W. Sample Lead Request Form 1 (DCIS to DCIS)
- X. Sample Lead Request Form 1 (DCIS to DCIO)
- Y. Sample Case Summary–Update Form 1
- Z. Sample Significant Incident Reporting Form 1 (Ex. 1–Indictment)
- AA. Sample Significant Incident Reporting Form 1 (Ex. 2–Indictment–Unsealed)
- BB. Sample Significant Incident Reporting Form 1 (Ex. 3–PLEA)
- CC. Sample Significant Incident Reporting Form 1 (Ex. 4–Sentencing)
- DD. Sample Significant Incident Reporting Form 1 (Ex. 5–Suspension)
- EE. Sample Report of Investigation (Prosecutorial Format)
- FF. Sample Report of Investigation (Condensed Format)
- GG. Sample Case Transfer Form 1 (Ex. 1)
- HH. Sample Case Transfer Form 1 (Ex. 2)
- II. Sample Case Reassignment Form 1
- JJ. Sample Case Termination Form 1 (Joint Agency ROI)
- KK. Sample Case Termination Form 1 (No ROI Submitted)
- LL. Sample Information Report Form 1 (Allegations Received But Are Not Pursued)
- MM. Sample Information Report/Referred Form 1
- NN. Sample Information Report/External Lead Response Form 1 (DCIO Lead Response)
- OO. Sample Information Report/Supplemental Information Form 1
- PP. Sample Audit Coordination Memorandum
- QQ. OGE Form 202 (Notification of Conflict of Interest Referral)
- RR. DCIS Form 5 (Case Review Record)
- SS. DCIS Form 5A (Case Review Continuation Page)

TT. DOJ Discovery Guidance on Criminal Procedures

UU. DCIS Form 4 (Case Closeout Checklist)

ATTACHMENT A

SAMPLE GENERIC FORM 1



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
DEFENSE CRIMINAL INVESTIGATIVE SERVICE
OFFICE NAME
OFFICE ADDRESS
CITY, STATE ZIP

[UID]-[OFFICE CODE]-[CASE CATEGORY CODE]

[REPORT DATE]

[CASE TITLE] (*Note: CIRs/IRs require a full case title, otherwise use abbreviated title*)

[WARNING STATEMENTS GO HERE – e.g. QUI TAM, GRAND JURY, UCO,
JUVENILE, RESTRICTED DISSEMINATION]

[INITIAL ENTRY/REPORT TITLE]: Narrative goes here...

CLASSIFICATION:

~~FOR OFFICIAL USE ONLY~~
~~LAW ENFORCEMENT SENSITIVE~~

DCIS Form 1 MAY 2017

WARNING

The information in this document marked FOUO-LES is the property of the Department of Defense Inspector General and may be distributed within the Federal Government (and its contractors) to law enforcement, public safety and protection, and intelligence officials and individuals with a need to know. Distribution to other entities without prior DoD IG authorization is prohibited. Precautions shall be taken to ensure this information is stored and destroyed in a manner that precludes unauthorized access. Information bearing the FOUO-LES marking may not be used in legal proceedings without prior authorization from the originator. Recipients are prohibited from posting information marked FOUO-LES on a website or unclassified network.

28-A-1
May 2017

ATTACHMENT A

[UID]-[OFFICE CODE]-[CASE CATEGORY CODE]

2

Prepared by: <Preparer, Office Code>

Approved by: <Approver, Office Code>

<Digitally sign above the line.>

<Digitally sign above the line.>

DISTR: [OFFICE CODE(S)]/[OTHER DISTRIBUTION]

CLASSIFICATION:

~~FOR OFFICIAL USE ONLY~~
~~LAW ENFORCEMENT SENSITIVE~~

DCIS Form 1 MAY 2017

WARNING

The information in this document marked FOUO-LES is the property of the Department of Defense Inspector General and may be distributed within the Federal Government (and its contractors) to law enforcement, public safety and protection, and intelligence officials and individuals with a need to know. Distribution to other entities without prior DoD IG authorization is prohibited. Precautions shall be taken to ensure this information is stored and destroyed in a manner that precludes unauthorized access. Information bearing the FOUO-LES marking may not be used in legal proceedings without prior authorization from the originator. Recipients are prohibited from posting information marked FOUO-LES on a website or unclassified network.

28-A-2
May 2017

ATTACHMENT E

CASE CATEGORY CODES

CATEGORY CODE	CATEGORY CODE DESCRIPTION
(b)(7)(E)	BRIBERY – OTHER
	BRIBERY – CONTRACTING OFFICIAL
	MISSION BRIEFING
	RECOVERY ACT BRIEFING
	RECOVERY ACT OUTREACH
	CONFLICT OF INTEREST – OTHER
	CONFLICT OF INTEREST – FINANCIAL
	CONFLICT OF INTEREST – EMPLOYMENT CONSIDERATIONS
	PAY & ALLOWANCE FRAUD – OTHER
	PAY & ALLOWANCE FRAUD – TRAVEL/PER DIEM
	PAY & ALLOWANCE FRAUD – PAYROLL
	PAY & ALLOWANCE FRAUD – WORKERS’ COMPENSATION FRAUD
	ANTITRUST ACT VIOLATION – OTHER
	ANTITRUST ACT VIOLATION – BID RIGGING
	ANTITRUST ACT VIOLATION – BID ROTATION
	ANTITRUST ACT VIOLATION – PRICE FIXING
	PROCUREMENT FRAUD – OTHER
	PROCUREMENT FRAUD – SUBSTITUTION/NON-CONFORMING PRODUCT
	PROCUREMENT - COUNTERFEIT PARTS/MATERIALS
	PROCUREMENT FRAUD – COST/LABOR MISCHARGING
	PROCUREMENT FRAUD – DEFECTIVE PRICING
	PROCUREMENT FRAUD – CONTRACTOR/SUBCONTRACTOR KICKBACKS
	REDISTRIBUTION/MARKETING FRAUD – OTHER
	INTERNAL INQUIRY – OTHER
	INTERNAL INQUIRY – DCIS PERSONNEL
	INTERNAL INQUIRY – OTHER OIG PERSONNEL
	COMMISSARY/SUBSISTENCE FRAUD – OTHER
	TRICARE FRAUD – OTHER
	TRICARE FRAUD – MEDICAL PRACTITIONER
	TRICARE FRAUD – HEALTH CARE FACILITY
	TRICARE FRAUD – HEALTH CARE KICKBACKS
	TRICARE FRAUD – PHARMACEUTICAL FRAUD
	THEFT/LARCENY/EMBEZZLEMENT – OTHER
	THEFT/LARCENY/EMBEZZLEMENT – PROPERTY/EQUIPMENT/SUPPLY
	THEFT/LARCENY/EMBEZZLEMENT – FUNDS/NEGOTIABLE INSTRUMENTS
	THEFT/LARCENY/EMBEZZLEMENT – SUSPICIOUS FINANCIAL TRANSACTIONS

ATTACHMENT E

CATEGORY CODE	CATEGORY CODE DESCRIPTION ¹
(b)(7)(E)	THEFT/LARCENY/EMBEZZLEMENT – GOVERNMENT OWNED WEAPONS SYSTEM HARDWARE
	THEFT/LARCENY/EMBEZZLEMENT – ADP/COMPUTER HARDWARE
	THEFT/LARCENY/EMBEZZLEMENT – SURPLUS PROPERTY/SCRAP
	THEFT/LARCENY/EMBEZZLEMENT – GOVERNMENT CHARGE CARD MISUSE
	THEFT/LARCENY/EMBEZZLEMENT – SUSPICIOUS FINANCIAL TRANSACTIONS
	THEFT/LARCENY – COMBAT – OTHER
	THEFT/LARCENY – COMBAT – FIREARMS
	THEFT/LARCENY – COMBAT – AMMUNITION
	THEFT/LARCENY – COMBAT – EXPLOSIVES, GRENADES, BOMBS
	GRATUITIES (GOVT OFFICIAL) – OTHER
	GRATUITIES (GOVT OFFICIAL) – CONTRACTING OFFICIAL
	COUNTER-PROLIFERATION VIOLATIONS – COMMERCIAL ITEMS/OTHER
	COUNTER-PROLIFERATION VIOLATIONS – TECHNOLOGY (INCLUDING COMPUTERS)/TECHNICAL PLANS AND DRAWINGS
	COUNTER-PROLIFERATION VIOLATIONS – GOVERNMENT OWNED ARMS/AMMUNITION/EXPLOSIVES
	COUNTER-PROLIFERATION VIOLATIONS – NUCLEAR MATERIAL
	COUNTER-PROLIFERATION VIOLATIONS – DUAL USE ITEMS WITH SIGNIFICANT DOD IMPACT
	PROGRAM MANAGEMENT IRREGULARITIES – OTHER
	PROGRAM MANAGEMENT IRREGULARITIES – CONTRACT ADMINISTRATION
	FORGERY OF NEGOTIABLE/OTHER INSTRUMENTS – OTHER
	ENVIRONMENTAL CRIMES – OTHER
	GENERAL CRIMINAL OFFENSES – OTHER (INCLUDES DRUG OFFENSES)
	CTIP – OTHER
	CTIP – FORCED LABOR/INVOLUNTARY SERVITUDE/DEBT BONDAGE
	CTIP – DOCUMENT TAMPERING
	CTIP – SEX TRAFFICKING
	COMPUTER CRIMES – OTHER
	COMPUTER CRIMES – INTRUSION
CATEGORY	CATEGORY CODE DESCRIPTION

(b)(7)(E)

ATTACHMENT E

CODE	
(b)(7)(E)	COMPUTER CRIMES – CHILD PORNOGRAPHY
	INSPECTION
	SECURITY VIOLATIONS – OTHER
	SECURITY VIOLATIONS – COMPROMISE OF CLASSIFIED
	SECURITY VIOLATIONS – CONTRACTUAL REQUIREMENTS
	OTHER OFFENSES – ALL OTHERS NOT DEFINED ELSEWHERE

ATTACHMENT F

CASE DISPOSITION CODES

DISPOSITION CODE	CASE DISPOSITION CODE DESCRIPTION
(b)(7)(E)	UNDER RESOURCED – DCIS Manpower UCO – Operation concluded PROJECT – Project concluded DECLINATION – Prosecution declined and no administrative action taken FINISHED – Culpability established and at least 1 (or more) subject(s) adjudicated; Administrative action taken INFORMATION REPORT – Referred to other organization or DCIS office SUSPENSE – ROI completed; awaiting adjudicative decision/response TRANSFERRED – Open case transferred to another DCIS office UNSUBSTANTIATED – Culpability not established and No adjudicative/administrative referral INFORMATION REPORT – Closed, without action or Outside Lead finished CANCELLED – Case cancelled prior to completion; No adjudicative/administrative referral

ATTACHMENT I
COMMON USE ACRONYMS & USE OF ABBREVIATIONS

COMMON USE ACRONYMS & USE OF ABBREVIATIONS

This document contains a list of commonly used acronyms and abbreviations found in DCIS reports.

Acronyms

The term “acronym” refers to a group of letters formed by combining the first letter or letters of several words. Acronyms are written without periods and are usually composed of all capital letters, although some exceptions exist, for example, DeCA. Use only acronyms that are in accepted use.

Establishing Acronyms

Some acronyms may be used without giving a written-out explanation of the words they represent. These acronyms can be used without first being spelled out.

DoD – Department of Defense
DoD IG – Department of Defense Inspector General
DCIS – Defense Criminal Investigative Service
FY – fiscal year
OIG – Office of Inspector General
SA – Special Agent
FBI – Federal Bureau of Investigation

Other acronyms will be spelled out first prior to use. To establish these acronyms, place the acronym in parentheses immediately following the spelling out of the word or phrase in the text for which it stands. Establish the acronym at first reference in *text*. Do not establish acronyms in headings or subheadings. Do not use an acronym in a heading or subheading unless it has been established previously in text.

The Defense Logistics Agency (DLA) requested assistance from the DCIS, Arlington Resident Agency, Arlington, VA.

Using Established Acronyms

Once you establish an acronym in the text (page 1 and after), you may use the same acronym throughout the report without reestablishing it. However, to aid readability, you may reestablish acronyms as needed in subsequent elements of the report.

Abbreviations

An abbreviation is a shortened form of a word or words and contains a period or periods. For the purposes of this guidance and our reports, we distinguish between an abbreviation (a short form

ATTACHMENT I

followed by a period) and an acronym (a short form not followed by a period). Avoid using abbreviations because abbreviations are often confusing to readers unfamiliar with the subject.

Avoid using abbreviations in the text. Generally, only the approved exceptions listed below are used in the text without explanation. If you must establish an abbreviation in the text, spell out the full term at first reference, followed by the abbreviation in parentheses.

Approved exceptions are a.m., D.C., No. (preceding a report number), p.m., St. (as in St. Louis and St. Paul), and U.S.

a.m. and p.m.

Use lowercase letters followed by periods when showing exact times. Do not use military time (for example, 2200 hours). Note in the following examples how whole hours are shown.

Note: Use the terms “midnight” and “noon” rather than clock time (12:00).

The photographs were taken at 10:45 a.m. and at noon January 25, 20XX, at Norfolk Naval Air Station, Virginia.

When we checked the files, we noted that the duty officer had signed the checklist on the safe at 11:00 p.m., not at midnight, as had been previously stated.

Cities and States

Spell out the names of cities. The two-letter acronym may be used, and is the preference, for States. Be consistent throughout the report or other document. For example, do not spell out the state in one paragraph and in another paragraph use the two letter acronym (e.g. Virginia vs. VA). When referring to Washington, District of Columbia, use “D.C.” for District of Columbia. Note that periods are used to separate the two letter acronym.

The contracting offices are in Vienna, VA, and Washington, D.C.

Months

Spell out the word “months” in the text. Do not separate the month and the year with a comma if no day is given.

We reviewed documentation dated from June 20XX through September 20XX.

The analysis report dated June 10, 2009, was provided to the Defense Contract Audit Agency.

Number, No.

ATTACHMENT I

Use the abbreviation “No.” preceding the numbers of circulars, bulletins, and reports.

Use the abbreviation “No.” as shown in the following examples.

OMB Circular No. A-123
OMB Bulletin No. 54

Department of Defense Inspector General Audit Report No. D-2001-001 was issued before DLA delegated the responsibility to DCMC.

Fiscal Year

The acronym FY is approved for references to a fiscal year (FY 20XX) without definition and without appearing on the acronym list. When used without a year (as a noun or adjective), spell out “fiscal year.” Always indicate when the year referred to is fiscal. Calendar year is assumed unless the year is preceded by FY. Do not use a hyphen to separate years.

Use the modifier “a” before “fiscal year,” but “an” before “FY.” This is based on the sound that FY makes, rather than the fact that it begins with a vowel. FY is pronounced “eff why”; therefore, it counts as a consonant sound.

Use of appropriated funds during a fiscal year that they are not needed does not meet the intent of the bona fide needs rule.

It was an FY 2009 appropriation.

GWOT

Global War on Terror. Remove this term from report titles. Replace GWOT with “Overseas Contingency Operations (OCO)” if objectives related to both Operation Enduring Freedom (OEF) and Operation Iraqi Freedom (OIF). If objectives related only to operations in Iraq, replace GWOT with OIF. If objectives related only to operations in Afghanistan, replace GWOT with OEF. If objectives extended to operations beyond Southwest Asia, specify locale, as in “operations in Afghanistan and Korea,” or wherever is applicable.

OTHER GUIDANCE

Word “Government”

When using the word Government to refer to the Federal Government, capitalize the “G.” When referring generically to foreign governments or State governments (such as the German government or the Texas State government), do not capitalize the “g.” The adjective “governmental” is not normally capitalized, as in “inherently governmental functions.”

Second References

Capitalize a word when establishing it as the short form for a long phrase or title.

ATTACHMENT I

when additional references will be made to the Act and short form is desired

The Competition in Contracting Act (the Act) requires full disclosure. The Act further states that

Directives, Instructions, and Regulations

When only one directive, instruction, or regulation is mentioned in a report, you can use the short form without its being formally established. Capitalize “Directive,” “Instruction,” and “Regulation” when using these terms in a short form.

first reference

DoD Directive 5010.40, “Managers’ Internal Control (MIC) Program Procedures,” January 4, 2006, states

second reference

The Directive refers

first reference

DoD Directive 5000.2, “Acquisition and Storage of War Reserves,” requires

second reference

The Directive states

ATTACHMENT I

Persons

Capitalize civilian, military, and professional titles immediately preceding a name.

President Bush	Ambassador Farrell	
Lieutenant Smith	Chairman Haney	the Honorable John Glenn

Do not capitalize titles of military officers or lower level officials used without their names.

The second lieutenant headed the division that processed forms.

The Defense Logistics Agency staff delegated the responsibility to the appropriate program executive officer and the administrative contracting officer.

The branch chief of the Los Angeles ADP review team stated that . . .

Business Entities

The common types of legal businesses can be abbreviated, as follows:

ABC Corporation or ABC CORP
ABC, Limited Liability Company or ABC, LLC
ABC, Limited Liability Partnership or ABC, LLP
ABC, Incorporated or ABC, INC.
ABC, Limited or ABC, LTD

ATTACHMENT J

SUGGESTED FORM 1 REPORT TITLES

- ADMINISTRATIVE ACTION/JOB TERMINATION
- ADMINISTRATIVE ACTION REFERRAL
- AUTHORIZED INVESTIGATIVE DEMAND RETURN
- AUTHORIZED INVESTIGATIVE DEMAND SERVICE
- CASE ASSUMPTION
- CASE INITIATION
- CASE REASSIGNMENT
- CASE REOPENING
- CASE SUMMARY *(note- subsequent updates will include the date)
- CASE TERMINATION
- CASE TRANSFER
- CONSENT SEARCH
- CONTRACT FILE REVIEW
- DISPOSITION OF EVIDENCE
- EVIDENCE SEIZURE
- FOIA REQUEST
- GRAND JURY SUBPOENA RETURN
- GRAND JURY SUBPOENA SERVICE
- HANDWRITING EXEMPLARS
- DODIG SUBPOENA SERVICE
- DODIG SUBPOENA RETURN

ATTACHMENT J

- INFORMATION REPORT
- INFORMATION REPORT/REFERRED
- INTERVIEW OF (WITNESS/SUBJECT NAME, ETC.)
- LABORATORY TESTING REQUEST
- LABORATORY TESTING RESULTS
- LEAD REQUEST
- LEAD RESPONSE
- PEN REGISTER
- PDD EXAMINATION REQUEST
- PROSECUTORIAL DECLINATION
- PROSECUTORIAL REFERRAL
- RECEIPT OF RECORDS FROM (Source of)
- RECORDS REVIEW
- REMOVAL OF SIC STATUS
- RETURN OF EVIDENCE
- RETURN OF RECORDS
- SEARCH WARRANT EXECUTION
- SIGNIFICANT INCIDENT/INDICTMENT
- SIGNIFICANT INCIDENT/FINAL FORFEITURE
- SIGNIFICANT INCIDENT/GUILTY PLEA
- SIGNIFICANT INCIDENT/SENTENCING

ATTACHMENT J

- SIGNIFICANT INCIDENT/SUSPENSION
- SIGNIFICANT INCIDENT/DEBARMENT
- STATUS CHANGE
- SUPPLEMENTAL INFORMATION
- SURVEILLANCE ACTIVITY
- TECHNICAL SERVICES REQUEST
- TITLE CHANGE

ATTACHMENT K

SPECIAL INTEREST CASE (SIC) FACTORS

SPECIAL INTEREST CASE FACTOR LISTING
SUSPECTED DEFECTIVE PRODUCT
AMERICAN RECOVERY AND REINVESTMENT ACT
OVERSEAS CONTINGENCY OPERATIONS
CONGRESSIONAL INQUIRY
SMALL BUSINESS INNOVATIVE RESEARCH/SMALL BUSINESS TECHNOLOGY TRANSFER
TRAFFICKING IN PERSONS
SENSITIVE INVESTIGATION
SUSPICIOUS ACTIVITY REPORTING (eGUARDIAN)

(Note: Sample entry for SIC Factor(s) section of the CIR, IR or Case Summary):

Special Interest Factor(s):

- AMERICAN RECOVERY AND REINVESTMENT ACT

(Note: If there are multiple SIC Factors, the entry should look as follows:

Special Interest Factor(s):

- CONGRESSIONAL INQUIRY
- OVERSEAS CONTINGENCY OPERATIONS

DOJ DISCOVERY GUIDANCE ON CRIMINAL PROCEDURES



U.S. Department of Justice

Office of the Deputy Attorney General

The Deputy Attorney General

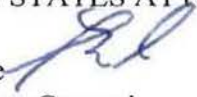
Washington, D.C. 20530

March 30, 2011

MEMORANDUM FOR THE ASSOCIATE ATTORNEY GENERAL AND
THE ASSISTANT ATTORNEYS GENERAL FOR THE
CRIMINAL DIVISION
NATIONAL SECURITY DIVISION
CIVIL RIGHTS DIVISION
ANTITRUST DIVISION
ENVIRONMENTAL AND NATIONAL RESOURCES DIVISION
TAX DIVISION

DIRECTOR, FEDERAL BUREAU OF INVESTIGATION
ADMINISTRATOR, DRUG ENFORCEMENT ADMINISTRATION
DIRECTOR, UNITED STATES MARSHALS SERVICE
PRINCIPAL DEPUTY DIRECTOR, BUREAU OF ALCOHOL,
TOBACCO, FIREARMS AND EXPLOSIVES
DIRECTOR, BUREAU OF PRISONS

ALL UNITED STATES ATTORNEYS

FROM: James M. Cole 
Deputy Attorney General

SUBJECT: Guidance on the Use, Preservation, and Disclosure of Electronic
Communications in Federal Criminal Cases

This memorandum supplements the January 4, 2010 Guidance for Prosecutors Regarding Criminal Discovery issued by Deputy Attorney General David W. Ogden (Ogden Memo), particularly section 1.B.5, Substantive Case-Related Communications, and is to be read in conjunction therewith.¹ The guidance contained herein is directed to all Department of Justice personnel and to all law enforcement personnel participating as members of a prosecution team.²

¹ For guidance concerning cases involving national security information, see Acting Deputy Attorney General Gary G. Grindler's September 29, 2010 memorandum, "Policy and Procedures Regarding the Government's Duty to Search for Discoverable Information in the Possession of the Intelligence Community or Military in Criminal Investigations."

² "Prosecution team" members include federal, state, and local law enforcement officers and other government officials participating in the investigation and prosecution of the criminal case against the defendant. USAM 9-5.001. The Ogden Memo provides additional guidance where state and local law enforcement has any involvement in a criminal case, stating:

MEMORANDUM TO DISTRIBUTION LIST

Page 2

Subject: Guidance on the Use, Preservation, and Disclosure of
Electronic Communications in Federal Criminal Cases

I. Summary

This memorandum provides guidance for prosecution team members on the use and preservation of electronic communications (“e-communications”). The basic principles are simple. Prosecution team members should think about the content of any e-communication before sending it; use appropriate language; think about whether e-communication is appropriate to the circumstances, or whether an alternative form of communication is more appropriate; and determine in advance how to preserve potentially discoverable information.

II. The Relationship Between the Government’s Legal Discovery Obligations, Department of Justice Discovery Policies, and This Guidance

The Government’s discovery obligations in federal criminal cases are set forth in constitutional case law, particularly *Brady v. Maryland*, 373 U.S. 83 (1963), and *Giglio v. United States*, 405 U.S. 150 (1972); the Jencks Act (18 U.S.C. 3500); Federal Rules of Criminal Procedure 16 and 26.2; and applicable rules of professional conduct.

Specific Department of Justice disclosure policies entitled Disclosure of Exculpatory and Impeachment Information (*Brady* policy) and Potential Impeachment Information Concerning Law Enforcement Witnesses (*Giglio* policy) are set forth in the United States Attorneys’ Manual (USAM) at Sections 9-5.001 and 9-5.100.

The purpose of this memorandum is to provide guidance to ensure that the Government meets its legal discovery obligations as applied to electronic communications.³ As used in this guidance, the term “e-communications” includes emails, text messages, SMS (short message service), instant messages, voice mail, pin-to-pin communications, social networking sites, bulletin boards, blogs, and similar means of electronic communication. This memorandum also provides guidance on how e-communications should and should not be used during the investigation and prosecution of a federal criminal case. A failure to comply with the guidance

In such cases, prosecutors should consider (1) whether state or local agents are working on behalf of the prosecutor or are under the prosecutor’s control; (2) the extent to which state and federal governments are part of a team, are participating in a joint investigation, or are sharing resources; and (3) whether the prosecutor has ready access to the evidence. Courts will generally evaluate the role of a state or local law enforcement agency on a case-by-case basis. Therefore, prosecutors should make sure they understand the law in their circuit and their office’s practice regarding discovery in cases in which a state or local agency participated in the investigation or on a task force that conducted the investigation.

Prosecutors are encouraged to err on the side of inclusiveness when identifying the members of the prosecution team for discovery purposes. Carefully considered efforts to locate discoverable information are more likely to avoid future litigation over *Brady* and *Giglio* issues and avoid surprises at trial.

³ This memorandum is solely intended to provide guidance to law enforcement personnel in order to attain compliance with the government’s criminal discovery obligations with regard to electronic communications. It does not create any right in any person or entity, and it is not enforceable in any criminal or civil case. *United States v. Caceres*, 440 U.S. 741 (1979).

MEMORANDUM TO DISTRIBUTION LIST

Page 3

Subject: Guidance on the Use, Preservation, and Disclosure of
Electronic Communications in Federal Criminal Cases

contained in this memorandum may result in delay, expense, and other consequences prejudicial to a prosecution, but it does not necessarily mean that there has been or will be a violation of a disclosure obligation.

III. Guidance for Achieving Full Compliance with the Government's Legal Discovery Obligations Relating to Electronic Communications

A. Benefits and Risks of E-communications

E-communications offer substantial benefits, including speed, sharing, and efficiency.

E-communications also present substantial risks. Because e-communications frequently are prepared and sent quickly and without supervisory review, they may not be as complete or accurate as more formal reports and may reflect a familiar or jovial tone. In court, defense counsel may try to use e-communications containing material inconsistencies, omissions, errors, incomplete statements, or jokes to impeach the credibility of a witness. Additionally, there is a risk that defense counsel will use poorly drafted e-communications between agents, witnesses, and/or prosecutors in court to create the false impression that they contain relevant or contradictory factual information. These risks can be particularly problematic in criminal prosecutions because, depending upon their content, e-communications may be discoverable under federal law.

Thus, prosecution team members should exercise the same care in generating case-related e-communications that they exercise when drafting more formal reports. All prosecution team members need to understand the risks of e-communications, the need to comply with agency rules regarding documentation and record-keeping during an investigation, the importance of careful and professional communication, and the obligation to preserve and produce such communications when appropriate.

B. Categories of E-communications

Case-related e-communications generally fall into four categories:

Substantive communications. "Substantive communications" include:

- factual information about investigative activity;
- factual information obtained during interviews or interactions with witnesses (including victims), potential witnesses, experts, informants, or cooperators;
- factual discussions related to the merits of evidence;

MEMORANDUM TO DISTRIBUTION LIST

Page 4

Subject: Guidance on the Use, Preservation, and Disclosure of Electronic Communications in Federal Criminal Cases

- factual information or opinions relating to the credibility or bias of witnesses, informants and potential witnesses;⁴ and
- other factual information that is potentially discoverable under *Brady*, *Giglio*, Rule 16, or Rule 26.2 (Jencks Act).

Substantive communications or the information within them may be discoverable.

Logistical communications. “Logistical communications” include e-communications that contain travel information; identify dates, times and locations of hearings or meetings; transmit reports; etc. Generally, logistical communications are not discoverable.

Privileged or protected communications. “Privileged communications” include attorney-client privileged communications, attorney work product communications, and deliberative process privileged communications.⁵ “Protected communications” are those covered by F.R.Crim.P. 16(a)(2).⁶ Generally, these communications are not discoverable so long as any discoverable facts contained in them are disclosed in other materials produced in discovery.

⁴ For example, if a prosecutor or agent opines that an informant will make a “bad” witness because the informant has made prior inconsistent statements, the opinion itself is core work product that need not be disclosed to the defense, but the prior inconsistent statements should be disclosed if the informant testifies at trial. See generally, Discovery BlueBook § 6.12.5, *Opinion or Reputation Evidence Regarding Veracity*.

⁵ Pursuant to applicable law, a privilege may apply to communications:

- a. between prosecutors on matters that require supervisory approval or legal advice, *e.g.*, prosecution memoranda, *Touhy* approval requests, *Giglio* requests, wire tap applications and reviews, and case strategy discussions;
- b. between prosecutors or agency counsel and other prosecuting office personnel, agents, or other agency personnel on case-related matters, including but not limited to organization, tasks that need to be accomplished, research, and analysis;
- c. between prosecutors and agency counsel or agency personnel (including agents) on legal issues relating to criminal cases, including, but not limited to, *Giglio* and *Touhy* requests; and
- d. from the prosecutor or agency counsel to an agent, other agency personnel, or prosecuting office personnel giving legal advice or requesting investigation of certain matters in anticipation of litigation (*e.g.*, “to-do” list).

If warranted, the sender of a privileged e-communication is encouraged to place a “privileged communication” warning on the communication to flag its privileged nature.

⁶See, generally, Discovery BlueBook 3.8, *Information Not Subject to Disclosure by the Government – Rule 16(a)(2)*.

MEMORANDUM TO DISTRIBUTION LIST

Page 5

Subject: Guidance on the Use, Preservation, and Disclosure of
Electronic Communications in Federal Criminal Cases

Mixed Communications. A communication that contains a mix of the categories above may be partially discoverable and may need careful review by a prosecutor or review by a court before a final determination is made as to whether it should be disclosed in discovery.⁷

C. Using E-communications

The following guidance applies at all phases of a criminal case including investigation, trial preparation, trial, and after trial:

1. Prosecution team members should discuss and make sure they understand the e-communications and discovery policies and guidance applicable to their case.
2. Prosecution team members should only write and send e-communications that they would feel comfortable being displayed to the jury in court or in the media.
3. Prosecution team members should be particularly cautious in any e-communications with potential witnesses who are not law enforcement personnel, taking care to avoid substantive e-communications. Of course, any potentially discoverable information should be preserved, regardless of whether the communication is written or oral.
4. Substantive e-communications among prosecution team members should be avoided except when, to meet operational needs, they are the most effective means of communication. Examples include where prosecution team members are in different countries or time zones, or where other operational imperatives require such e-communications. Prosecution team members should consider whether a formal report would be a better way of ensuring accurate communication, clarifying a matter, or preserving potentially discoverable information. Again, potentially discoverable information should be preserved, regardless of whether the communication is written or oral.
5. Prosecution team members may use e-communications for logistical communications, for example, to schedule meetings with witnesses, agents, prosecutors, or other members of the prosecution team, or to transmit a formal report. However, prosecution team members should avoid including any substantive information in such e-communications.

⁷ For e-communications containing information to be produced in discovery, a prosecutor may make appropriate redactions, summarize the substance of an e-communication in a letter rather than disclosing the e-communication itself, seek a protective order, or take other safeguarding measures.

MEMORANDUM TO DISTRIBUTION LIST

Page 6

Subject: Guidance on the Use, Preservation, and Disclosure of
Electronic Communications in Federal Criminal Cases

6. E-communications, like formal reports, should state facts accurately and completely; be professional in tone; and avoid witticism, careless commentary, opinion, or over-familiarity. E-communications should maintain and accurately reflect an arms-length relationship with potential witnesses who are not law enforcement personnel, including victims and informants.
7. Prosecution team members ordinarily should not include information in an e-communication that must be incorporated into a formal agency report, especially with regard to witness interviews or other communications containing a witness's or agent's factual recitations. If for some reason substantive case-related information must be contained in an e-communication, prosecution team members should ensure that the information is accurate and is included in any formal report required by agency policies. Material inconsistencies between an e-communication and a formal report, or omissions, errors, or incomplete statements in e-communications, may be impeachment information and may be used in cross-examination in court proceedings.
8. Prosecution team members should limit the subject matter of any e-communication to a single case at a time to make it easier to segregate e-communications by case.
9. Prosecution team members should inform individuals not on the prosecution team but otherwise involved in the case, including victims, witnesses, and outside experts, that e-communications are a written record that might be disclosed to the defendant and used for impeachment in court like any other written record.
10. Prosecution team members must comply with any applicable policies governing e-communications and should not use personally-owned electronic communication devices, personal email accounts, social networking sites, or similar accounts to transmit or post case-related information.
11. Prosecution team members should not post case-related or sensitive agency information on a non-agency website or social networking site. Information posted on publically accessible websites or social networking sites may be used to impeach the author.
12. Prosecution team members should send e-communications only to those individuals who have a need to know the information contained in the communication.

MEMORANDUM TO DISTRIBUTION LIST

Page 7

Subject: Guidance on the Use, Preservation, and Disclosure of
Electronic Communications in Federal Criminal Cases

13. Prosecution team members should employ practices that will preserve any potentially discoverable information contained in e-communications. Preservation of e-communications in certain messaging formats (e.g., text, SMS, instant, PIN, etc.) may present unique challenges.⁸ At present, the approaches to preserving potentially discoverable information in e-communications may include: incorporating any potentially discoverable information into a comprehensive report, capturing the message in some format that can be made available to the prosecutor, or preserving the e-communication itself. These approaches may evolve as technology changes and technical capabilities change.
14. The sender should notify recipients of any restrictions on forwarding e-communications that the sender wants observed.

D. Preservation of E-communications

There are three steps to proper handling of e-communications in criminal cases: preservation,⁹ review, and disclosure. The number of e-communications preserved and reviewed likely will be greater than the number ultimately produced as discovery.

1. Who is responsible for preserving e-communications?

Each potentially discoverable e-communication should be preserved by each member of the prosecution team who is either (a) the creator/sender/forwarder of the e-communication, or (b) a primary addressee (*i.e.*, in the “To” line). If no member of the prosecution team is a sender or primary addressee of a substantive e-communication (*e.g.*, if an agent is cc’d on an email by a witness to a third party), then each member of the prosecution team who is a secondary addressee (*i.e.*, a “cc” or “bcc” recipient) should preserve the email. Although in some instances this practice will lead to preserving multiple copies of the same e-communication, it will ensure preservation.

2. When should e-communications be preserved?

To ensure that e-communications are properly preserved, prosecution team members should move and/or copy potentially discoverable e-communications, together with any potentially discoverable attachments and threads of related e-communications, from the user’s e-

⁸ Each component should provide guidance to affected employees on how to preserve the various messaging formats (text, SMS, IM, PIN, etc.), or any other e-communication that may contain potentially discoverable information. Where an e-communication containing potentially discoverable information cannot be preserved electronically or printed, the agency’s inability to do so should be documented so that the preservation approach can be explained in court.

⁹ This guidance is concerned only with the Government’s criminal discovery obligations. It is not intended to address the requirements of the Federal Records Act, 44 U.S.C. §§ 3101 *et seq.*

MEMORANDUM TO DISTRIBUTION LIST

Page 8

Subject: Guidance on the Use, Preservation, and Disclosure of
Electronic Communications in Federal Criminal Cases

communication account¹⁰ to a secure permanent or semi-permanent storage location associated with the investigation and prosecution, or print and place them with the criminal case file as soon as possible but not later than 10 days after the e-communication is sent or received. Prosecution team members should ensure that such preservation occurs before the agency computer system automatically deletes the e-communication because of storage limitations or retention policies. Designated network locations that are not subject to automatic deletion may be a secure storage location for potentially discoverable e-communications.

3. Which e-communications should be preserved for later review?

During an investigation it is difficult to know which e-communications may be discoverable if the case is charged. Therefore, members of the prosecution team should err on the side of preservation when deciding which e-communications to preserve for review.

The following e-communications should be preserved for later review and possible disclosure to the defendant:

- Substantive e-communications created or received in the course of an investigation and prosecution.
- All e-communications sent to or received from potential witnesses who are not law enforcement personnel regardless of content.
- E-communications that contain both potentially privileged and unprivileged substantive information.

As discussed below in section II.E.2, agents and their supervisors should work with prosecutors to identify all e-communications that are particularly sensitive and deserve careful consideration before any determination is made to provide them to the defendant as discovery.

4. Which e-communications do not need to be preserved for later review?

Logistical communications between prosecution team members, *e.g.*, scheduling meetings or assigning tasks, generally do not need to be preserved and made available to the prosecutor for review because they are not discoverable unless something in their content suggests they should be disclosed under *Brady*, *Giglio*, *Jencks* or Rule 16.

¹⁰ With respect to emails, this includes the user's inbox, sent items, and deleted items.

MEMORANDUM TO DISTRIBUTION LIST

Page 9

Subject: Guidance on the Use, Preservation, and Disclosure of
Electronic Communications in Federal Criminal Cases

5. How should e-communications be preserved?

When possible, e-communications should be preserved in their native electronic format to enable efficient discovery review. Otherwise, they should be printed and preserved.¹¹ E-communications that cannot be printed should be preserved in some other fashion, *e.g.*, a narrative report. For email, creation of electronic folders into which pertinent emails can be easily moved is the recommended method for preservation in native format.

6. How do parallel civil or administrative investigations/proceedings affect which e-communications should be preserved in a criminal case?

The best practices for parallel criminal, civil, and administrative proceedings vary from case to case. Be aware that civil proceedings may have different or broader preservation requirements; therefore, the prosecution team should consult with the lawyers handling the parallel proceedings for guidance on preserving e-communications in the early stages of parallel proceedings.

E. Reviewing and Producing Discoverable E-communications to the Defendant

1. Responsibilities of the Prosecutor

It is the prosecutor's responsibility to oversee the gathering, review and production of discovery.¹² In determining what will be disclosed in discovery, the prosecutor should ensure that each e-communication is evaluated, taking into consideration, among other things, what facts are reported, the author, whether the author will be a witness, whether it is inconsistent with other e-communications or formal reports, and whether it reflects bias, contains impeachment information, or contains any information (regardless of credibility or admissibility) that appears inconsistent with any element of the offense or the Government's theory of the case.

If the e-communication contains any particularly sensitive information (as described below), then the prosecutor should consider whether to file a motion for a protective order, seek supervisory approval to delay disclosure (in accordance with USAM § 9-5.001), make appropriate redactions, summarize the substance of an e-communication in a letter rather than disclosing the e-communication itself, or take other safeguarding measures.

¹¹ Agencies may require some e-communications to be printed to paper to comply with the Federal Records Act. Notwithstanding paper copies, preserving e-communications in native electronic format still is appropriate, when feasible, to facilitate electronic review and to preserve metadata that, in rare circumstances, may be discoverable.

¹² When dealing with voluminous e-communications, the prosecution team should discuss and plan for a substantial lead time to gather and review the materials.

MEMORANDUM TO DISTRIBUTION LIST

Page 10

Subject: Guidance on the Use, Preservation, and Disclosure of
Electronic Communications in Federal Criminal Cases

2. Responsibilities of the Prosecution Team

It is the responsibility of each member of the prosecution team to make available to the prosecutor all potentially discoverable e-communications so that the prosecutor can review them to determine what should be produced in discovery. The discovery obligation continues throughout the case. *See* Fed.R. Crim. P. 16(c).

Prosecution team members who submit potentially discoverable e-communications to the prosecutor should identify e-communications that deserve especially careful scrutiny by the prosecutor. For example, prosecution team members should identify e-communications the disclosure of which could:

- affect the safety of any person,
- reveal sensitive investigative techniques,
- compromise the integrity of another investigation, or
- reveal national security information.

165 Guidance for Prosecutors Regarding Criminal Discovery

January 4, 2010

MEMORANDUM FOR DEPARTMENT PROSECUTORS

FROM: David W. Ogden
Deputy Attorney General

SUBJECT: Guidance for Prosecutors Regarding Criminal Discovery

The discovery obligations of federal prosecutors are generally established by Federal Rules of Criminal Procedure 16 and 26.2, 18 U.S.C. § 3500 (the Jencks Act), *Brady v. Maryland*, 373 U.S. 83 (1963), and *Giglio v. United States*, 405 U.S. 150 (1972). In addition, the United States Attorney's Manual describes the Department's policy for disclosure of exculpatory and impeachment information. See [USAM 9-5.001](#). In order to meet discovery obligations in a given case, Federal prosecutors must be familiar with these authorities and with the judicial interpretations and local rules that discuss or address the application of these authorities to particular facts. In addition, it is important for prosecutors to consider thoroughly how to meet their discovery obligations in each case. Toward that end, the Department has adopted the guidance for prosecutors regarding criminal discovery set forth below. The guidance is intended to establish a methodical approach to consideration of discovery obligations that prosecutors should follow in every case to avoid lapses that can result in consequences adverse to the Department's pursuit of justice. The guidance is subject to legal precedent, court orders, and local rules. It provides prospective guidance only and is not intended to have the force of law or to create or confer any rights, privileges, or benefits. See *United States v. Caceres*, 440 U.S. 741 (1979).

The guidance was developed at my request by a working group of experienced attorneys with expertise regarding criminal discovery issues that included attorneys from the Office of the Deputy Attorney General, the United States Attorneys' Offices, the Criminal Division, and the National Security Division. The working group received comment from the Office of the Attorney General, the Attorney General's Advisory Committee, the Criminal Chiefs Working Group, the Appellate Chiefs Working Group, the Professional Responsibility Advisory Office, and the Office of Professional Responsibility. The working group produced this consensus document intended to assist Department prosecutors to understand their obligations and to manage the discovery process.

By following the steps described below and being familiar with laws and policies regarding discovery obligations, prosecutors are more likely to meet all legal requirements, to make considered decisions about disclosures in a particular case, and to achieve a just result in every case. Prosecutors are reminded to consult with the designated criminal discovery coordinator in their office when they have questions about the scope of their discovery obligations. Rules of Professional Conduct in most jurisdictions also impose ethical obligations on prosecutors regarding discovery in criminal cases. Prosecutors are also reminded to contact the Professional Responsibility Advisory Office when they have questions about those or any other ethical responsibilities.

Department of Justice Guidance for Prosecutors Regarding Criminal Discovery

Step 1: Gathering and Reviewing Discoverable Information[[FN1](#)]

A. Where to look—The Prosecution Team

Department policy states:

28-TT-11
May 2017

It is the obligation of federal prosecutors, in preparing for trial, to seek all exculpatory and impeachment information from all members of the prosecution team. Members of the prosecution team include federal, state, and local law enforcement officers and other government officials participating in the investigation and prosecution of the criminal case against the defendant.

[USAM 9-5.001](#). This search duty also extends to information prosecutors are required to disclose under Federal Rules of Criminal Procedure 16 and 26.2 and the Jencks Act.

In most cases, "the prosecution team" will include the agents and law enforcement officers within the relevant district working on the case. In multi-district investigations, investigations that include both Assistant United States Attorneys and prosecutors from a Department litigating component or other United States Attorney's Office (USAO), and parallel criminal and civil proceedings, this definition will necessarily be adjusted to fit the circumstances. In addition, in complex cases that involve parallel proceedings with regulatory agencies (SEC, FDIC, EPA, etc.), or other non-criminal investigative or intelligence agencies, the prosecutor should consider whether the relationship with the other agency is close enough to make it part of the prosecution team for discovery purposes.

Some factors to be considered in determining whether to review potentially discoverable information from another federal agency include:

- Whether the prosecutor and the agency conducted a joint investigation or shared resources related to investigating the case;
- Whether the agency played an active role in the prosecution, including conducting arrests or searches, interviewing witnesses, developing prosecutorial strategy, participating in targeting discussions, or otherwise acting as part of the prosecution team;
- Whether the prosecutor knows of and has access to discoverable information held by the agency;
- Whether the prosecutor has obtained other information and/or evidence from the agency;
- The degree to which information gathered by the prosecutor has been shared with the agency;
- Whether a member of an agency has been made a Special Assistant United States Attorney;
- The degree to which decisions have been made jointly regarding civil, criminal, or administrative charges; and
- The degree to which the interests of the parties in parallel proceedings diverge such that information gathered by one party is not relevant to the other party.

Many cases arise out of investigations conducted by multi-agency task forces or otherwise involving state law enforcement agencies. In such cases, prosecutors should consider (1) whether state or local agents are working on behalf of the prosecutor or are under the prosecutor's control; (2) the extent to which state and federal governments are part of a team, are participating in a joint investigation, or are sharing resources; and (3) whether the prosecutor has ready access to the evidence. Courts will generally evaluate the role of a state or local law enforcement agency on a case-by-case basis. Therefore, prosecutors should make sure they understand the law in their circuit and their office's practice regarding discovery in cases in which a state or local agency participated in the investigation or on a task force that conducted the investigation.

Prosecutors are encouraged to err on the side of inclusiveness when identifying the members of the prosecution team for discovery purposes. Carefully considered efforts to locate discoverable information are more likely to avoid future litigation over *Brady* and *Giglio* issues and avoid surprises at trial.

Although the considerations set forth above generally apply in the context of national security investigations and prosecutions, special complexities arise in that context. Accordingly, the Department expects to issue additional guidance for such cases. Prosecutors should begin considering potential discovery obligations early in an investigation that has national security implications and should also carefully evaluate their discovery obligations prior to filing charges. This evaluation should consider circuit and district precedent and include consultation with national security experts in their own offices and in the National Security Division.

B. What to Review

To ensure that all discovery is disclosed on a timely basis, generally all potentially discoverable material within the custody or control of the prosecution team should be reviewed.[FN2] The review process should cover the following areas:

1. The Investigative Agency's Files: With respect to Department of Justice law enforcement agencies, with limited exceptions,[FN3] the prosecutor should be granted access to the substantive case file and any other file or document the prosecutor has reason to believe may contain discoverable information related to the matter being prosecuted. [FN4] Therefore, the prosecutor can personally review the file or documents or may choose to request production of potentially discoverable materials from the case agents. With respect to outside agencies, the prosecutor should request access to files and/or production of all potentially discoverable material. The investigative agency's entire investigative file, including documents such as FBI Electronic Communications (ECs), inserts, emails, etc. should be reviewed for discoverable information. If such information is contained in a document that the agency deems to be an "internal" document such as an email, an insert, an administrative document, or an EC, it may not be necessary to produce the internal document, but it will be necessary to produce all of the discoverable information contained in it. Prosecutors should also discuss with the investigative agency whether files from other investigations or non-investigative files such as confidential source files might contain discoverable information. Those additional files or relevant portions thereof should also be reviewed as necessary.

2. Confidential Informant (CI)/Witness (CW)/Human Source (CHS)/Source (CS) Files: The credibility of cooperating witnesses or informants will always be at issue if they testify during a trial. Therefore, prosecutors are entitled to access to the agency file for each testifying CI, CW, CHS, or CS. Those files should be reviewed for discoverable information and copies made of relevant portions for discovery purposes. The entire informant/source file, not just the portion relating to the current case, including all proffer, immunity, and other agreements, validation assessments, payment information, and other potential witness impeachment information should be included within this review.

If a prosecutor believes that the circumstances of the case warrant review of a non-testifying source's file, the prosecutor should follow the agency's procedures for requesting the review of such a file.

Prosecutors should take steps to protect non-discoverable, sensitive information found within a CI, CW, CHS, or CS file. Further, prosecutors should consider whether discovery obligations arising from the review of CI, CW, CHS, and CS files may be fully discharged while better protecting government or witness interests such as security or privacy via a summary letter to defense counsel rather than producing the record in its entirety.

Prosecutors must always be mindful of security issues that may arise with respect to disclosures from confidential source files. Prior to disclosure, prosecutors should consult with the investigative agency to evaluate any such risks and to develop a strategy for addressing those risks or minimizing them as much as possible, consistent with discovery obligations.

3. Evidence and Information Gathered During the Investigation: Generally, all evidence and information gathered during the investigation should be reviewed, including anything obtained during searches or via subpoenas, etc. As discussed more fully below in Step 2, in cases involving a large volume of potentially discoverable information, prosecutors may discharge their disclosure obligations by choosing to make the voluminous information available to the defense.

4. Documents or Evidence Gathered by Civil Attorneys and/or Regulatory Agency in Parallel Civil Investigations: If a prosecutor has determined that a regulatory agency such as the SEC is a member of the prosecution team for purposes of defining discovery obligations, that agency's files should be reviewed. Of course, if a regulatory agency is not part of the prosecution team but is conducting an administrative investigation or proceeding involving the same subject matter as a criminal investigation, prosecutors may very well want to ensure that those files are reviewed not only to locate discoverable information but to locate inculpatory information that may advance the criminal case. Where there is an ongoing parallel civil proceeding in which Department civil attorneys are participating, such as a qui tam case, the civil case files should also be reviewed.

5. Substantive Case-Related Communications: "Substantive" case-related communications may contain discoverable information. Those communications that contain discoverable information should be maintained in the case file

or otherwise preserved in a manner that associates the investigation. "Substantive" case-related communications are most likely to occur (1) among prosecutors and/or agents, (2) between prosecutors and/or agents and witnesses and/or victims, and (3) between victim/witness coordinators and witnesses and/or victims.

Such communications may be memorialized in emails, memoranda, or notes. "Substantive" communications include factual reports about investigative activity, factual discussions of the relative merits of evidence, factual information obtained during interviews or interactions with witnesses/victims, and factual issues relating to credibility.

Communications involving case impressions or investigative or prosecutive strategies without more would not ordinarily be considered discoverable, but substantive case-related communications should be reviewed carefully to determine whether all or part of a communication (or the information contained therein) should be disclosed.

Prosecutors should also remember that with few exceptions (see, e.g., Fed.R.Crim.P. 16(a)(1)(B)(ii)), the format of the information does not determine whether it is discoverable. For example, material exculpatory information that the prosecutor receives during a conversation with an agent or a witness is no less discoverable than if that same information were contained in an email. When the discoverable information contained in an email or other communication is fully memorialized elsewhere, such as in a report of interview or other document(s), then the disclosure of the report of interview or other document(s) will ordinarily satisfy the disclosure obligation.

6. Potential Giglio Information Relating to Law Enforcement Witnesses: Prosecutors should have candid conversations with the federal agents with whom they work regarding any potential *Giglio* issues, and they should follow the procedure established in [USAM 9-5.100](#) whenever necessary before calling the law enforcement employee as a witness. Prosecutors should be familiar with circuit and district court precedent and local practice regarding obtaining *Giglio* information from state and local law enforcement officers.

7. Potential Giglio Information Relating to Non-Law Enforcement Witnesses and Fed.R.Evid. 806 Declarants: All potential *Giglio* information known by or in the possession of the prosecution team relating to non-law enforcement witnesses should be gathered and reviewed. That information includes, but is not limited to:

- Prior inconsistent statements (possibly including inconsistent attorney proffers, *see United States v. Triumph Capital Group*, 544 F.3d 149 (2d Cir. 2008))
- Statements or reports reflecting witness statement variations (see below)
- Benefits provided to witnesses including:
 - Dropped or reduced charges
 - Immunity
 - Expectations of downward departures or motions for reduction of sentence
 - Assistance in a state or local criminal proceeding
 - Considerations regarding forfeiture of assets
 - Stays of deportation or other immigration status considerations
 - S-Visas
 - Monetary benefits
 - Non-prosecution agreements
 - Letters to other law enforcement officials (e.g. state prosecutors, parole boards) setting forth the extent of a witness's assistance or making substantive recommendations on the witness's behalf
 - Relocation assistance
 - Consideration or benefits to culpable or at risk third-parties
- Other known conditions that could affect the witness's bias such as:
 - Animosity toward defendant
 - Animosity toward a group of which the defendant is a member or with which the defendant is affiliated
 - Relationship with victim
 - Known but uncharged criminal conduct (that may provide an incentive to curry favor with a prosecutor)

- Prior actS under Fed.R.Evid. 608
- Prior convictions under Fed.R.Evid. 609
- Known substance abuse or mental health issues or other issues that could affect the witness's ability to perceive and recall events

8. Information Obtained in Witness Interviews: Although not required by law, generally speaking, witness interviews[FN5] should be memorialized by the agent.[FN6] Agent and prosecutor notes and original recordings should be preserved, and prosecutors should confirm with agents that substantive interviews should be memorialized. When a prosecutor participates in an interview with an investigative agent, the prosecutor and agent should discuss note-taking responsibilities and memorialization before the interview begins (unless the prosecutor and the agent have established an understanding through prior course of dealing). Whenever possible, prosecutors should not conduct an interview without an agent present to avoid the risk of making themselves a witness to a statement and being disqualified from handling the case if the statement becomes an issue. If exigent circumstances make it impossible to secure the presence of an agent during an interview, prosecutors should try to have another office employee present. Interview memoranda of witnesses expected to testify, and of individuals who provided relevant information but are not expected to testify, should be reviewed.

- Witness Statement Variations and the Duty to Disclose: Some witnesses' statements will vary during the course of an interview or investigation. For example, they may initially deny involvement in criminal activity, and the information they provide may broaden or change considerably over the course of time, especially if there are a series of debriefings that occur over several days or weeks. Material variances in a witness's statements should be memorialized, even if they are within the same interview, and they should be provided to the defense as *Giglio* information.
- Trial Preparation Meetings with Witnesses: Trial preparation meetings with witnesses generally need not be memorialized. However, prosecutors should be particularly attuned to new or inconsistent information disclosed by the witness during a pre-trial witness preparation session. New information that is exculpatory or impeachment information should be disclosed consistent with the provisions of [USAM 9-5.001](#) even if the information is first disclosed in a witness preparation session. Similarly, if the new information represents a variance from the witness's prior statements, prosecutors should consider whether memorialization and disclosure is necessary consistent with the provisions of subparagraph (a) above.
- Agent Notes: Agent notes should be reviewed if there is a reason to believe that the notes are materially different from the memorandum, if a written memorandum was not prepared, if the precise words used by the witness are significant, or if the witness disputes the agent's account of the interview. Prosecutors should pay particular attention to agent notes generated during an interview of the defendant or an individual whose statement may be attributed to a corporate defendant. Such notes may contain information that must be disclosed pursuant to Fed.R.Crim.P. 16(a)(1)(A)-(C) or may themselves be discoverable under Fed.R.Crim.P. 16(a)(1)(B). *See, e.g., United States v. Clark*, 385 F.3d 609, 619-20 (6th Cir. 2004) and *United States v. Vaffee*, 380 F.Supp.2d 11, 12-14 (D. Mass. 2005).

Step 2: Conducting the Review

Having gathered the information described above, prosecutors must ensure that the material is reviewed to identify discoverable information. It would be preferable if prosecutors could review the information themselves in every case, but such review is not always feasible or necessary. The prosecutor is ultimately responsible for compliance with discovery obligations. Accordingly, the prosecutor should develop a process for review of pertinent information to ensure that discoverable information is identified. Because the responsibility for compliance with discovery obligations rests with the prosecutor, the prosecutor's decision about how to conduct this review is controlling. This process may involve agents, paralegals, agency counsel, and computerized searches. Although prosecutors may delegate the process and set forth criteria for identifying potentially discoverable information, prosecutors should not delegate the disclosure determination itself. In cases involving voluminous evidence obtained from third parties, prosecutors should consider providing defense access to the voluminous documents to avoid the possibility that a well-intentioned review process nonetheless fails to identify material discoverable evidence. Such broad disclosure may not be feasible

in national security cases involving classified informat

Step 3: Making the Disclosures

The Department's disclosure obligations are generally set forth in Fed.R.Crim.P. 16 and 26.2, 18 U.S.C. § 3500 (the Jencks Act), *Brady*, and *Giglio* (collectively referred to herein as "discovery obligations"). Prosecutors must familiarize themselves with each of these provisions and controlling case law that interprets these provisions. In addition, prosecutors should be aware that [USAM 9-5.001](#) details the Department's policy regarding the disclosure of exculpatory and impeachment information and provides for broader disclosures than required by *Brady* and *Giglio*. Prosecutors are also encouraged to provide discovery broader and more comprehensive than the discovery obligations. If a prosecutor chooses this course, the defense should be advised that the prosecutor is electing to produce discovery beyond what is required under the circumstances of the case but is not committing to any discovery obligation beyond the discovery obligations set forth above.

- A. Considerations Regarding the Scope and Timing of the Disclosures: Providing broad and early discovery often promotes the truth-seeking mission of the Department and fosters a speedy resolution of many cases. It also provides a margin of error in case the prosecutor's good faith determination of the scope of appropriate discovery is in error. Prosecutors are encouraged to provide broad and early discovery consistent with any countervailing considerations. But when considering providing discovery beyond that required by the discovery obligations or providing discovery sooner than required, prosecutors should always consider any appropriate countervailing concerns in the particular case, including, but not limited to: protecting victims and witnesses from harassment or intimidation; protecting the privacy interests of witnesses; protecting privileged information; protecting the integrity of ongoing investigations; protecting the trial from efforts at obstruction; protecting national security interests; investigative agency concerns; enhancing the likelihood of receiving reciprocal discovery by defendants; any applicable legal or evidentiary privileges; and other strategic considerations that enhance the likelihood of achieving a just result in a particular case. In most jurisdictions, reports of interview (ROIs) of testifying witnesses are not considered Jencks material unless the report reflects the statement of the witness substantially verbatim or the witness has adopted it. The Working Group determined that practices differ among the USAOs and the components regarding disclosure of ROIs of testifying witnesses. Prosecutors should be familiar with and comply with the practice of their offices.

Prosecutors should never describe the discovery being provided as "open file." Even if the prosecutor intends to provide expansive discovery, it is always possible that something will be inadvertently omitted from production and the prosecutor will then have unintentionally misrepresented the scope of materials provided. Furthermore, because the concept of the "file" is imprecise, such a representation exposes the prosecutor to broader disclosure requirements than intended or to sanction for failure to disclose documents, e.g. agent notes or internal memos, that the court may deem to have been part of the "file." When the disclosure obligations are not clear or when the considerations above conflict with the discovery obligations, prosecutors may seek a protective order from the court addressing the scope, timing, and form of disclosures.

- B. Timing: Exculpatory information, regardless of whether the information is memorialized, must be disclosed to the defendant reasonably promptly after discovery. Impeachment information, which depends on the prosecutor's decision on who is or may be called as a government witness, will typically be disclosed at a reasonable time before trial to allow the trial to proceed efficiently. See [USAM 9-5.001](#). Section 9-5.001 also notes, however, that witness security, national security, or other issues may require that disclosures of impeachment information be made at a time and in a manner consistent with the policy embodied in the Jencks Act. Prosecutors should be attentive to controlling law in their circuit and district governing disclosure obligations at various stages of litigation, such as pre-trial hearings, guilty pleas, and sentencing.

Prosecutors should consult the local discovery rules for the district in which a case has been indicted. Many districts have broad, automatic discovery rules that require Rule 16 materials to be produced without a request by the defendant and within a specified time frame, unless a court order has been entered delaying discovery, as is common in complex cases. Prosecutors must comply with these local rules, applicable case law, and any final court order regarding discovery. In the absence of guidance from such local rules or court orders, prosecutors should consider making Rule 16 materials available as soon as is reasonably practical but must make disclosure no later than a reasonable time before trial. In deciding when and in what format to provide discovery, prosecutors should always consider security concerns and the other factors set

forth in subparagraph (A) above. Prosecutors should also ensure that they disclose Fed.R.Crim.P. 16(a)(1)(E) materials in a manner that triggers the reciprocal discovery obligations in Fed.R.Crim.P. 16(b)(1).

Discovery obligations are continuing, and prosecutors should always be alert to developments occurring up to and through trial of the case that may impact their discovery obligations and require disclosure of information that was previously not disclosed.

- C. Form of Disclosure: There may be instances when it is not advisable to turn over discoverable information in its original form, such as when the disclosure would create security concerns or when such information is contained in attorney notes, internal agency documents, confidential source documents, Suspicious Activity Reports, etc. If discoverable information is not provided in its original form and is instead provided in a letter to defense counsel, including particular language, where pertinent, prosecutors should take great care to ensure that the full scope of pertinent information is provided to the defendant.

Step 4: Making a Record

One of the most important steps in the discovery process is keeping good records regarding disclosures. Prosecutors should make a record of when and how information is disclosed or otherwise made available. While discovery matters are often the subject of litigation in criminal cases, keeping a record of the disclosures confines the litigation to substantive matters and avoids time-consuming disputes about what was disclosed. These records can also be critical when responding to petitions for post-conviction relief, which are often filed long after the trial of the case. Keeping accurate records of the evidence disclosed is no less important than the other steps discussed above, and poor records can negate all of the work that went into taking the first three steps.

Conclusion

Compliance with discovery obligations is important for a number of reasons. First and foremost, however, such compliance will facilitate a fair and just result in every case, which is the Department's singular goal in pursuing a criminal prosecution. This guidance does not and could not answer every discovery question because those obligations are often fact specific. However, prosecutors have at their disposal an array of resources intended to assist them in evaluating their discovery obligations including supervisors, discovery coordinators in each office, the Professional Responsibility Advisory Office, and online resources available on the Department's intranet website, not to mention the experienced career prosecutors throughout the Department. And, additional resources are being developed through efforts that will be overseen by a full-time discovery expert who will be detailed to Washington from the field. By evaluating discovery obligations pursuant to the methodical and thoughtful approach set forth in this guidance and taking advantage of available resources, prosecutors are more likely to meet their discovery obligations in every case and in so doing achieve a just and final result in every criminal prosecution. Thank you very much for your efforts to achieve those most important objectives.

FN 1. For the purposes of this memorandum, "discovery" or "discoverable information" includes information required to be disclosed by Fed.R.Crim.P. 16 and 26.2, the Jencks Act, *Brady*, and *Giglio*, and additional information disclosable pursuant to [USAM 9-5.001](#).

FN 2. How to conduct the review is discussed below.

FN 3. Exceptions to a prosecutor's access to Department law enforcement agencies' files are documented in agency policy, and may include, for example, access to a non-testifying source's files.

FN 4. Nothing in this guidance alters the Department's Policy Regarding the Disclosure to Prosecutors of Potential Impeachment Information Concerning Law Enforcement Agency Witnesses contained in [USAM 9-5.100](#).

FN 5. "Interview" as used herein refers to a formal question and answer session with a potential witness conducted for the purpose of obtaining information pertinent to a matter or case. It does not include conversations with a potential witness for the purpose of scheduling or attending to other ministerial matters. Potential witnesses may provide substantive information outside of a formal interview, however. Substantive, case-related communications are addressed above.

FN 6. In those instances in which an interview was audio or video recorded, further memorialization will generally not be necessary.

[added January 2010] [cited in [USAM 9-5.001](#); [9-5.100](#)]

CHAPTER 30

DEFENSE CRIMINAL INVESTIGATIVE SERVICE ALTERNATIVE WORK SCHEDULES PROGRAM

<u>Contents</u>	<u>Section</u>
Purpose	30.1.
Reference	30.2.
Policies	30.3.
Part-Time Position for the 1811 Series Employee	30.4.

30.1. Purpose. This chapter supplements Department of Defense Inspector General Regulation (IGDR) 1400.610, “Alternative Work Schedules Program,” dated January 1, 1998, and contains policies for implementation of the Regulation. This chapter also implements the requirements and policies for the 1811 series part-time position.

30.2. Reference. IGDR 1400.610, “Alternative Work Schedules Program,” January 1, 1998 (available on the intranet).

30.3. Policies

30.3.a. **Nonagent Personnel.** All provisions of the Regulation apply to nonagent personnel.

30.3.b. Special Agent Personnel

30.3.b.(1). The provisions of Chapters 1 and 2 of the Regulation apply to all special agent personnel.

30.3.b.(2). Special agent personnel receiving Law Enforcement Availability Pay (LEAP) under Chapter 54 of the Special Agents Manual (SAM) may request a flexitour or gliding schedule as described in Chapter 3 of the Regulation. The credit hour provision of a flexitour or gliding schedule is not available to special agents receiving LEAP; however, special agents may receive overtime pay for all hours of work in excess of 8 hours in a day or 40 hours in a week that are ordered officially in advance by management. Any request for overtime must first be approved in advance by the Deputy Inspector General for Investigations. The Compressed Work Schedule (Chapter 4) provisions of the Regulation do not apply to special agents receiving LEAP.

30.3.b.(3). The Flexible Work Schedules (Chapter 3) (both flexitour schedule and gliding schedule) and Compressed Work Schedule (Chapter 4) provisions of the Regulation apply to special agent personnel who have voluntarily opted out of LEAP under SAM Chapter 54.

30.4. Part-Time Position for the 1811 Series Employee. The Office of the Inspector General of the Department of Defense allows for the 1811 series employee to work in a part-time position. The eligibility requirements, compensation, work hours, benefits, and procedures for the part-time position are set out in Attachment A.

ATTACHMENT A
REQUIREMENTS AND POLICIES
FOR THE 1811 SERIES EMPLOYEE PART-TIME POSITION

1. Eligibility Requirements

- a. Demonstrate a compelling reason.
- b. Be working at a “Fully Successful” level of performance.
- c. Part-time status will be approved on a yearly basis and will normally be limited to 5 years total as an Office of the Inspector General of the Department of Defense criminal investigator, regardless of the number of instances.
- d. All special agents are eligible for the program to the degree that the needs of the office and the Agency are consistent with participation in the program.

NOTE: The decision process will consider all facts and circumstances of the special agent’s request, as well as principles of good management in terms of resources and other concerns.

2. Compensation, Work Hours, and Benefits

- a. Rates of Pay. Part-time special agents are paid at the hourly rate of their current grade and step while in the program. This hourly rate includes any locality pay that may be applicable.
- b. Law Enforcement Availability Pay will not be paid to part-time special agents.
- c. Part-time schedules are between 16-32 hours per week and are established during the decision process by the supervisor.
- d. Part-time special agents should not normally be scheduled to work overtime. If a particular assignment (court appearance, trial) requires the part-time special agent to work more hours than those he/she is scheduled to work, adjustments in the work schedule, credit hours or appropriate compensation will be allowed.
- e. Overtime does not apply to a part-time special agent until he/she has worked 40 hours in a workweek.
- f. Leave accrual will be prorated based upon the employee’s length of service and hours in pay status, consistent with OPM regulations; benefit costs will be prorated based upon the particulars of the work schedule as well. Employees considering part-time employment should be aware of the following.

(1) Those in part-time work schedules are in a separate competitive level from other similarly classified positions for purposes of Reduction in Force.

(2) For purposes of demonstrating qualifications for promotion or reassignment, time in a part-time position is calculated as a percentage of the required 52 weeks of full-time (40 hours) experience (e.g., an employee on a 20-hour a week schedule will have to work 2 years to meet the qualification requirements for promotion in most circumstances).

g. Part-time employment does not affect an employee's retirement eligibility. Therefore, the mandatory retirement age is 57 years with 20 years of 1811 series experience. However, as mandated by the Part-time Employment Act, the amount of an 1811 series employee's accrued annuity will be prorated, under both the Civil Service Retirement System (CSRS) and the Federal Employee Retirement System (FERS).

h. Part-time special agents will not be authorized a Government vehicle on a domicile-to-duty basis.

3. Procedures

A written request with the eligibility requirements listed shall be submitted to the first line supervisor. The request must go through the chain of command. The Special Agent in Charge shall submit a concurrence or nonconcurrence to the Deputy Inspector General for Investigations for approval or disapproval. The Special Agent in Charge, Internal Operations, will initiate an SF 52, "Request for Personnel Action," requesting this action.

NOTE: Information needed in the written request:

- a. Provide in detail the reason for the request.
- b. Start date of the part-time status.
- c. Estimated ending date of the part-time status.



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

July 25, 2017
Ref: DODOIG-2017-000193

SENT VIA EMAIL

This is an interim response to your Freedom of Information Act (FOIA) request for a copy of the Defense Criminal Investigative Service (DCIS) Special Agents Manual. We received your request on December 31, 2016, and assigned it case number DODIG-2017-000193.

The Defense Criminal Investigative Service conducted a search and found the enclosed documents, which consist of Chapters 31 through 45 of the Special Agents Manual, as responsive to your request. After carefully reviewing the records, I have determined that 136 pages of records are appropriate for release in full, copies of which are enclosed. Additionally, I have determined that 40 pages of records are appropriate for release in part, and that 14 pages of records are exempt from disclosure pursuant to:

- 5 U.S.C. § 552 (b)(5), which pertains to certain inter-and intra-agency communications protected by the deliberative process privilege;
- 5 U.S.C. § 552 (b)(6), which pertains to information, the release of which would constitute a clearly unwarranted invasion of personal privacy;
- 5 U.S.C. § 552 (b)(7)(C), which pertains to records or information compiled for law enforcement purposes, the release of which could reasonably be expected to constitute an unwarranted invasion of personal privacy;
- 5 U.S.C. § 552 (b)(7)(E), which pertains to records or information compiled for law enforcement purposes, the release of which would disclose techniques and procedures for law enforcement investigations or prosecutions; and
- 5 U.S.C. § 552 (b)(7)(F), which pertains to records or information compiled for law enforcement purposes, the release of which could reasonably be expected to endanger the life or physical safety of any individual.

July 25, 2017
Ref: DODOIG-2017-000193

In view of the above interim response, you may consider this to be an adverse determination that may be appealed within 90 days of the date of this letter, however we recommend that you wait to submit any appeal until after a final response is sent to you. If you choose to appeal the interim release now, the appeal must be sent to the Department of Defense, Office of Inspector General, ATTN: FOIA Appellate Authority, Suite 10B24, 4800 Mark Center Drive, Alexandria, VA 22350-1500, postmarked within 90 days of this letter, and reference the file number above. I recommend that your appeal and its envelope both bear the notation "Freedom of Information Act Appeal." Please be assured that you retain the right to appeal our final determination and, when we provide our final response, you will be afforded another 90 calendar days in which to appeal.

You may seek dispute resolution services and assistance with your request from the DoD OIG FOIA Public Liaison Officer at 703-604-9785, or the Office of Government Information Services (OGIS) at 877-684-6448, ogis@nara.gov, or <https://ogis.archives.gov/>. Please note that OGIS mediates disputes between FOIA requesters and Federal agencies as a non-exclusive alternative to litigation. However, OGIS does not have the authority to mediate requests made under the Privacy Act of 1974 (request to access one's own records.)

Please note that this office is continuing to process your FOIA request, and you will be provided responses on a rolling basis. If you have any questions regarding this matter, please contact Searle Slutzkin at 703-699-7520 or via email at foiarequests@dodig.mil.

Sincerely,



Mark Dorgan
Division Chief
FOIA, Privacy and Civil Liberties Office

Enclosure(s):
As stated

CHAPTER 32
DEFENSE CRIMINAL INVESTIGATIVE SERVICE
MISSION BRIEFS

<u>Contents</u>	<u>Section</u>
Purpose	32.1.
Policy	32.2.
Training Goals	32.3.
Briefing Contents	32.4.
Responsibilities	32.5.
Conducting the Briefing	32.6.
Reporting Requirements	32.7.
Closing Comments	32.8.

32.1. Purpose

32.1.a. The purpose of this chapter is to establish policies, responsibilities, and procedures for administering the Defense Criminal Investigative Service (DCIS) Mission Brief Program. This program was formerly known as the DCIS Fraud and Integrity Awareness Training Program.

32.1.b. The focus of the DCIS Mission Brief is to increase the awareness of DoD employees to criminal activity within the Department such as terrorism, illegal technology transfer, product substitution, and public corruption; and to educate them on the mission of DCIS, its accomplishments in past criminal investigations, and its investigative priorities. Additionally, the DCIS Mission Brief is the primary method to educate non-Government employees, prospective applicants, other law enforcement agencies, and the public to increase their understanding of the DCIS mission. A secondary purpose of the DCIS Mission Brief is to increase the awareness of DoD employees to the possibility of bribe offers and the proper procedures to use in reporting those offenses to DCIS. The DCIS Mission Brief is intended to make the employee aware of the responsibilities of the Office of the Inspector General of the Department of Defense (OIG DoD); to understand the mission and investigative priorities of DCIS; to emphasize responsibilities with respect to prompt reporting of criminal activity within the Department; and to provide the appropriate knowledge of how to handle bribe offers, as well as how to recognize and report such instances of public corruption. These briefings are not intended to be a substitute for the Standards of Conduct Briefing, which is the responsibility of management to provide to their employees.

32.1.c. The DCIS Mission Brief should be conducted with a target audience of Government and contractor procurement officials, legal counsels, Agency heads, auditors, law enforcement officials, and other individuals in key management positions throughout DoD. Additionally, the DCIS Mission Brief should be tailored for presentation at professional conferences and trade shows, job fair presentations for potential applicants, and other instances when educating the targeted audience on the DCIS mission is the intended result.

32.1.d. The DCIS Mission Brief program provides a proactive method for the local DCIS office to obtain and develop a conduit to different DoD activities, professional law enforcement and procurement organizations, and colleges and universities in their area of investigative responsibility. It should be tailored and focused to encourage the free flow of information concerning possible illegal or improper activities affecting DoD, the interest of potential job applicants, and the sharing of information within the law enforcement community at local, state, and Federal levels.

32.2. Policy. DCIS Special Agents will conduct the presentations in all field elements, with specific focus on the following:

32.2.a. OIG DoD responsibilities and the DCIS mission,

32.2.b. emphasis on the employee's responsibility for prompt reporting of criminal activity within the Department, and

32.2.c. dissemination of OIG DoD policy concerning the handling of bribe offers.

32.3. Training Goals

32.3.a. Emphasize the DCIS mission and its investigative priorities.

32.3.b. Highlight DCIS adjudicative results and prosecutions of crimes against the Government and DoD for the purpose of deterring future criminal activity as it relates to DCIS investigative priorities.

32.3.c. Make DoD employees more aware of the possibilities of bribe offers and other public corruption activities, as well as their responsibilities for reporting such an activity once they know of it.

32.3.d. Emphasize to all DoD employees that the Standards of Conduct apply to all DoD employees, regardless of their position, grade, or rank.

32.4. Briefing Contents

32.4.a. The goals of the DCIS Mission Brief are identified in section 32.3. However, the specifics of the materials used to meet the training goals are left to the special agent making the presentation. This allows that special agent to tailor the briefing to the audience to whom he/she is speaking. Since the briefing should be tailored to the audience, the briefing special agent should contact an appropriate individual at the activity where the briefing is to be given in order to obtain information regarding the duties, grades, and other pertinent information concerning those to be briefed. This information can then be used to prepare a more effective briefing. A Microsoft PowerPoint presentation is available via the OIG intranet on the Investigations Admin Toolbox. This PowerPoint presentation is maintained and updated on a quarterly basis and may be edited for content to tailor the briefing to the targeted audience, with emphasis on the goals outlined in section 32.3.

32.4.b. The "DCIS Mission Brief" digitized video disk (DVD) can be used to deliver the briefing to a wide audience, to obtain information about the topics to be covered during the briefing, or in a "kiosk" fashion during a professional conference or job recruitment fair. Additionally, the DoD Hotline can provide posters and informational cards regarding the Hotline Program as a tool to

educate the audience and encourage reporting of criminal misconduct. Such items, along with the DCIS informational brochure available via the Office of Communications and Congressional Liaison (OCCL), may be used to effectuate the goals and purposes of the DCIS Mission Brief. Each DCIS office is encouraged to maintain a supply of these items. Requests should be submitted to the Special Agent in Charge, Internal Operations (SAC-INT).

32.5. Responsibilities

32.5.a. Each field element is encouraged to use all available resources, such as the OIG DoD Semiannual Report to Congress, Executive Summaries, Integrity Alert Bulletins, Indicators of Fraud in DoD Procurement Bulletins, and Fraud Vulnerability Reports that support the DCIS Mission Brief. The field elements are encouraged to forward any training and advertising material that may be of interest to other field elements to the SAC-INT, who will coordinate disseminating the materials to other field elements for their use in conducting the DCIS Mission Brief.

32.5.b. The SAC, Investigative Operations (SAC-INV), and the SAC-INT will, when appropriate, perform research and studies and provide summaries of lessons learned from actual criminal cases to supplement the training materials.

32.5.c. Each field office (FO) SAC will determine the requirements for the DCIS Mission Brief through liaison contacts within his/her geographic area of responsibility. Additionally, the FO SAC will be responsible for planning, scheduling, and presenting briefings to DoD field elements, potential job applicants, and the law enforcement community at local, state, and Federal levels.

32.6. Conducting the Briefing

32.6.a. The size of the audience can have a great effect on the ability of the briefing agent to provide an effective presentation. It is therefore recommended that, whenever possible, the audience size be kept relatively small. While one briefing to a large audience may initially appear to be more time-efficient, it may not reach everyone in the audience and in the long run may be less effective.

32.6.b. As these briefings may generate questions from the audience, structure the briefing to provide a question and answer session. Make every effort to provide the audience with answers to their questions, even if it entails taking the name and telephone number of the questioner so that an appropriate answer can be provided later.

32.7. Reporting Requirements. Information concerning the DCIS Mission Brief must be entered into the “Briefings” section of the Investigative Data System (IDS) for the accurate collection, storage, and retrieval of statistical data relating to DCIS activities. All data entry into the IDS will be made in accordance with the specific instructions contained in Chapter 50 of the DCIS Special Agents Manual (SAM). With respect to the unique identification number for the DCIS Mission Brief, it will be obtained in the same manner as any other case pursuant to SAM Chapter 50.

32.8. Closing Comments. Briefings are the first step in maintaining a free flow of information between the briefed activity or individual contacted and the DCIS office. Continued and ongoing liaison can provide greater opportunities to develop sources of information concerning illegal or improper activities that have an impact on DoD.

CHAPTER 33

RADIO COMMUNICATIONS

<u>Contents</u>	<u>Section</u>
Applicability and Scope	33.1.
Radio Communications	33.2.
Radio Terms Defined	33.3.
National Law Enforcement Communication Center (NLECC)	33.4.
Security of the DCIS Radio	33.5.
Radio Frequencies	33.6.
Use of the DCIS Radio	33.7.
Radio Call Signs and Communication Procedures	33.8.
Loan of DCIS Radios	33.9.
Maintenance of DCIS Radios	33.10.
Lost or Missing Radios	33.11.

33.1. Applicability and Scope

33.1.a. The provisions of this chapter apply to all Special Agents (SAs) and support personnel within DCIS and any personnel assigned to DCIS on a temporary basis.

33.1.b. This chapter provides the guidelines for the management and responsibilities of the DCIS Land Mobile Radio (LMR) communications program.

33.1.c. Headquarters, DCIS Technical Services Program is responsible for overseeing the DCIS LMR communications program.

33.2. Radio Communications. LMRs use a variety of LMR communications hardware. Within DCIS these devices include handheld two-way Very High Frequency (VHF) radios and radio repeaters.

(b)(7)(E)

(b)(7)(E)

33.3. Radio Terms Defined. The following radio-specific terms are defined with regard to DCIS LMR communications.

33.3.a. **Duplex Operation.** LMR communication whereby a radio transmits at one programmed frequency and receives on a secondary frequency. This is normally used for transmissions to and from stationary repeater sites. The use of a stationary repeater allows LMR users a greater area of coverage due to its greater power output and the height of the antenna.

33.3.b. **Simplex Operation.** LMR communication from one handheld or mobile radio to another, commonly referred to as point to point or line of sight, using a single programmed frequency.

33.3.c. **Talk Around.** A simplex LMR operation using the transmission and reception signal on the output frequency of the repeater. It allows for localized tactical operations of limited geographic scope (e.g., surveillance). It enables users to receive strategic communications without interfering with the repeater.

33.3.d. **OTAR (over-the-air rekeying).** The process of receiving an encryption key that is updated (b)(7)(E)

33.4. National Law Enforcement Communication Center. The Department of Homeland Security (DHS) provides access to DCIS and other law enforcement agencies to the National Law Enforcement Communication Center (NLECC), a nationwide radio communications network. It consists of hundreds of radio repeaters deployed throughout the United States. A majority of the repeaters are connected via telecommunications links to centrally monitored stations at the NLECC in Orlando, FL. Maps showing the locations and frequencies/channels (called NET by NLECC) of the CHARLIE 100 repeaters can be viewed on the S drive (S:\DCIS\Technical Services\Radios).

33.4.a. **CHARLIE 100.** CHARLIE 100 is the radio call sign used by the console operators at NLECC. CHARLIE 100 is staffed with 24-hour full-time console operators who provide services including:

- 33.4.a.(1).
- 33.4.a.(2).
- 33.4.a.(3).
- 33.4.a.(4).
- 33.4.a.(5).
- 33.4.a.(6).

(b)(7)(E)

- 33.4.a.(7).
- 33.4.a.(8).

(b)(7)(E)

33.5. Security of the DCIS Radio. DCIS radios are valuable items of Technical Investigative Equipment (TIE) and must be protected accordingly. Radios are also communications hardware that must be accessible whenever a SA is performing (or likely to be recalled to) investigative duties.

(b)(7)(E)

(b)(7)(E)

33.5.a. **Storage.** Radios should not be stored where they are susceptible to extreme conditions, such as high heat or moisture. While not in use, the radio should remain in a charger. If not protected, the radio could lose the shadow key or the entire programming load.

33.5.b. **Battery Care.** Batteries should remain charged at all times. Never allow a discharged battery to sit for an extended period. This can cause the battery to fully discharge and reverse polarity, which will render the battery unusable. Batteries should be recharged/refreshed at least once a month. This is accomplished by leaving your radio on and out of the charger until the voltage gets low enough for the radio to shut down automatically. Then place the radio back in the charger.

(b)(7)(E)

(b)(7)(E)

33.6. Radio Frequencies. Headquarters, DCIS Technical Services Program will conduct all programming of DCIS radios. On occasion, the program manager, DCIS Technical Services Program, may authorize individual DCIS offices to use other agencies or vendors to program DCIS LMR.

33.6.a. In addition to the NLECC frequencies programmed into DCIS LMR, there are several other frequencies assigned to DCIS. Several federal, state, and local law enforcement agencies have authorized DCIS SAs to operate on their individually assigned frequencies.

33.6.b. DCIS LMRs are also programmable to receive the frequencies used in the transmission of consensual body-wire transmitters.

33.6.c. The Federal Communications Commission (FCC) has set aside frequencies within the VHF high band for use as law enforcement mutual assistance. These frequencies are programmed into all DCIS LMR.

33.6.d. The National Oceanic and Atmospheric Administration (NOAA) receives only channels that have been programmed into all DCIS LMR.

33.6.e. DCIS has entered into MOUs with state and local law enforcement agencies allowing DCIS SAs to operate on frequencies specifically assigned to those investigative agencies. The DCIS requirements for each of these MOU agreements vary. To ensure the continued inoperability access to these frequencies, DCIS will operate on the frequencies only in exigent circumstances or when operationally involved in joint investigative activities supporting the agency assigned the LMR frequency being used.

33.7. Use of the DCIS Radio. The DCIS radio is to be used for official communications

during official daily activities, investigative activities (e.g., surveillance, search warrants, arrest warrants), and training. Maintain a minimum safe distance of at least 300 feet when using LMR near construction areas where explosives are used (e.g., road construction in mountainous areas) and around hospitals, as the radio frequency energy transmitted from the radio could interfere with the operation of critical hospital equipment. DCIS managers are responsible for ensuring all assigned SAs receive training on the proper use of DCIS LMR. The DCIS Technical Services Program is available to accomplish this training telephonically or through VTC when requested. The training should include the following procedures and operational doctrines.

33.7.a. General radio operation (powering the radios, changing channels and zones, push-to-talk procedures, etc.).

33.7.b. OTAR (when possible).

33.7.c. Proper communications with CHARLIE 100 (when possible).

33.7.d. Proper internal DCIS communication via DCIS handheld radios.

33.7.e. Phonetic alphabet.

33.7.f. CHARLIE 100's standard 10-series codes. (See paragraph 33.8.d.)

33.7.g. Never use profanity while communicating on the radio.

33.7.h. Do not retransmit nonofficial communications (e.g., music) on the radio.

33.7.i. Keep transmission concise and professional.

33.7.j. Do not attempt to block other transmissions.

33.7.k. Emergencies have priority. If someone on a frequency declares an emergency, uninvolved agents should stay off that frequency until the emergency is cleared. Attempts to access that frequency will interfere with efforts to provide assistance to the one in need.

33.7.l. Multiple parties use the same frequencies and expect to communicate without interference. When accessing a radio frequency, listen for a moment and look for the red transmission light, which indicates someone else is transmitting. If no one is transmitting, then key the microphone to transmit.

33.8. Radio Call Signs and Communication Procedures

(b)(7)(E)

(b)(7)(E)

33.8.c. **Range.** A radio's range is limited. The distance depends on the power of the radio and will not exceed the line of sight of the antenna. A radio installed in a vehicle has significantly greater power (0 watts vs. 5 watts), which increases the range of the handheld radio. Transmissions are sometimes garbled or difficult to understand. An SA may enhance communication by:

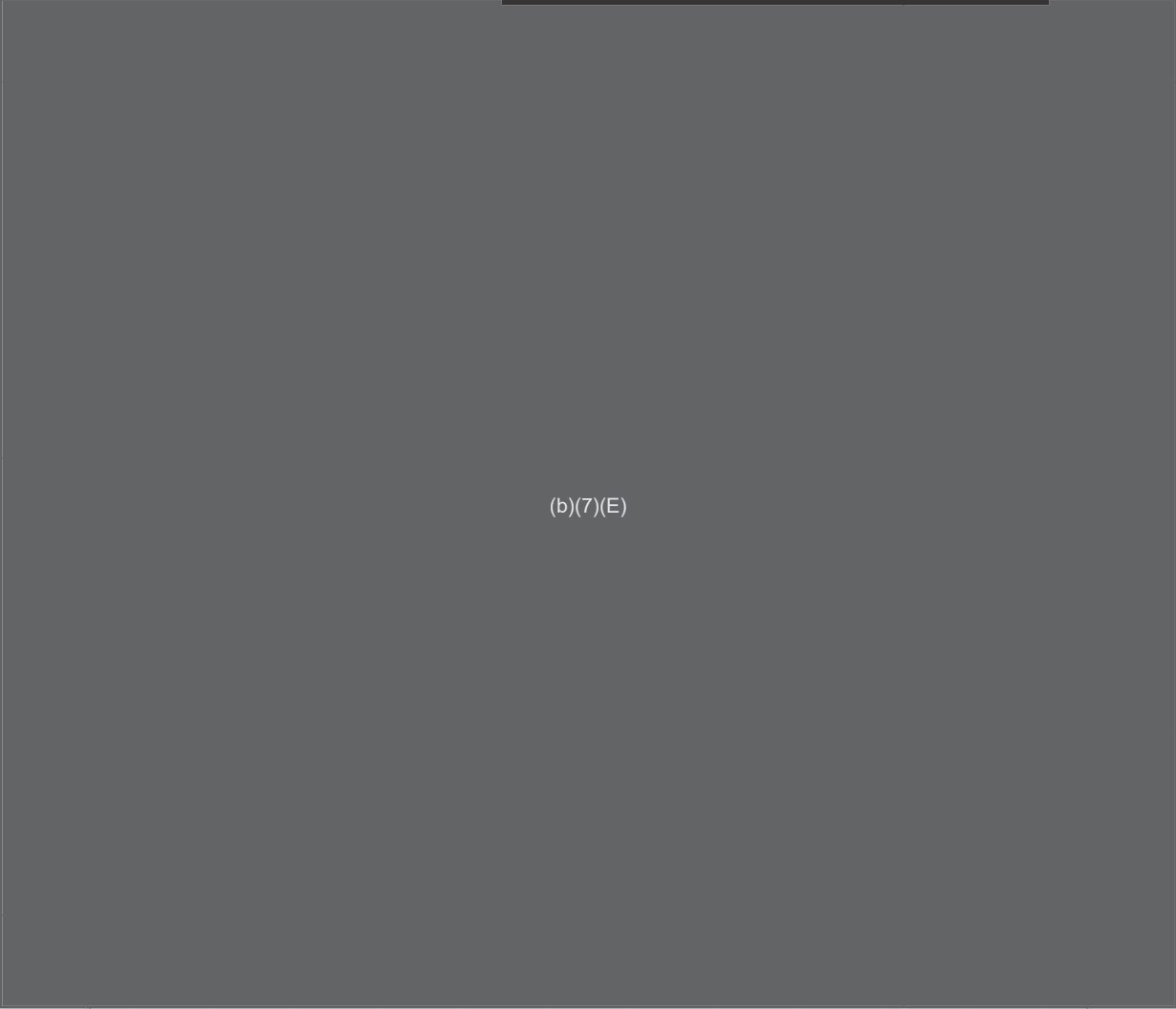
33.8.c.(1). increasing the line of sight by moving to a higher position (e.g., hilltop, higher building floor);

33.8.c.(2). moving toward moist ground or a body of water;

33.8.c.(3). moving away from obstructions (e.g., tall buildings); or

33.8.c.(4). avoiding valleys, power lines, steel structures, underpasses, and leafy trees.

33.8.d. **Ten Code.** Use plain language to get the message across with a minimum of time. However, some standard radio responses have been incorporated into a numeric code commonly referred to as the "ten code." (b)(7)(E)



(b)(7)(E)

33.8.e. **International Phonetic Alphabet.** The clarity of the words transmitted over the radio is sometimes difficult to understand. This is especially true when transmitting letters (e.g., license plates). Radio operators have developed a phonetic alphabet consisting of one word beginning with each letter of the alphabet. The International Phonetic Alphabet is:

A = Alpha
B = Bravo
C = Charlie
D = Delta
E = Echo
F = Foxtrot
G = Golf
H = Hotel
I = India

J = Juliet
K = Kilo
L = Lima
M = Mike
N = November
O = Oscar
P = Papa
Q = Quebec
R = Romeo

S = Sierra
T = Tango
U = Uniform
V = Victor
W = Whiskey
X = X-ray
Y = Yankee
Z = Zulu

Any of the standard law enforcement phonetic alphabets can be substituted for the international one. When in doubt, any word that clearly identifies the alphabet letter may be used.

33.8.f. Emergencies

33.8.f.(1). If an SA needs emergency assistance, he/she should state: "I have an emergency situation!" This alerts all parties that an emergency exists and serves to clear the frequency for specific requests for assistance.

33.8.f.(2). In plain language, the SA should identify himself or herself and location and describe the nature of the emergency. **(Remember that CHARLIE 100 is in Orlando, FL, and may not be familiar with your local area).**

33.8.f.(3). When using the Customs and DCIS frequencies in an emergency, CHARLIE 100 assumes control of the frequency. CHARLIE 100 will notify the appropriate emergency services (e.g., local police, ambulance, fire) to render assistance.

33.8.f.(4). Once the situation is under control, the SA should immediately declare the emergency over. CHARLIE 100 will continue to treat the situation as an emergency until told otherwise. It will also continue to provide an emergency response even though the condition has stabilized.

33.9. Loan of DCIS Radios. DCIS LMR may be lent to personnel of other law enforcement agencies when operationally necessary or during multiagency training and with DCIS manager (Special Agent in Charge, Assistant Special Agent in Charge, or Resident Agent in Charge) approval. However, the LMR will be returned to DCIS control immediately on completion of the operation or training exercise. LMR will not be loaned to non-law enforcement personnel. The radio allows access to encrypted law enforcement communications, and under agreements with Customs and other agencies, DCIS cannot grant LMR communication access to non-law enforcement personnel.

33.10. Maintenance of DCIS LMR. The DCIS Technical Operations Program is responsible for the repair and replacement of all DCIS radios. It is important to note that some software used to program DCIS radios is not industry-standard, and attempts to use non-DCIS software may render the radio unusable. Malfunctioning handheld radios must be returned to Headquarters, DCIS Technical Services Program for reprogramming and repair. The address to ship radios for repair or replacement can be found in the "Technical Services Contact Information" document on the S drive (S:\DCIS\Technical Services). If the radio does not work, try the following.

33.10.a. Check the battery status.

33.10.b. Check to see that the radio is set to the proper channel.

33.10.c. Check the encryption status. A radio set to operate in the encrypted mode will be able to receive a transmission in the clear. Two radios operating in the encrypted mode with different encryption keys will not be able to communicate.

33.10.d. Reset the radio by turning it off, waiting a few seconds, and then turning it on again. This will reset the logic and memory system.

33.10.e. Check the antenna connections.

33.10.f. Move to a location with better reception.

33.11. Lost or Missing Radios. The loss of any radio containing active DES-XL encryption poses a serious threat to communications security. CHARLIE 100 has procedures to ensure the encryption code does not become compromised if a DCIS radio is lost, stolen, or missing. To ensure this procedure is effective, a lost, stolen, or missing radio must be reported to DCIS Technical Services Program within 24 hours of discovery of the loss. Forward a Memorandum for Record (MFR) to the Special Agent in Charge, Investigative Operations Directorate, via the respective field office Special Agent in Charge. If the radio is assigned to a Headquarters SA, notify the respective program director of the circumstances within 2 business weeks. A copy of the MFR should be forwarded to the program manager, DCIS Technical Services Program, for inventory purposes.

CHAPTER 36
MOTOR VEHICLES

<u>Contents</u>	<u>Section</u>
Purpose	36.1.
References	36.2.
Authorization	36.3.
Assignment	36.4.
Acquisition	36.5.
Motor Vehicle Control Officers	36.6.
Authorized Drivers and Reporting Requirements	36.7.
Motor Vehicle Identification	36.8.
Motor Vehicle Registration	36.9.
Official Use of Motor Vehicles	36.10.
Domicile-to-Duty Transportation	36.11.
Carpooling	36.12.
Passengers in Government Furnished Vehicles	36.13.
Parking of Motor Vehicles	36.14.
Use of Government Furnished Vehicles in Lieu of Privately Owned Vehicles	36.15.
Use of Commercially Rented Motor Vehicles	36.16.
Use of Motor Vehicles by Non-DCIS Personnel	36.17.
Theft and Vandalism	36.18.
Safety and Accident Prevention	36.19.
Alcohol and Drug Use	36.20.
Motor Vehicle Accidents	36.21.
Investigation of Accidents/Theft/Vandalism	36.22.
Accident or Unsafe Practice Drug Testing	36.23.
Claims	36.24.
Maintenance, Repairs, and Services	36.25.
Administrative Control of Credit Cards	36.26.
Cash Purchases in Lieu of Credit Cards	36.27.
Vehicle Management Reporting Procedures	36.28.
Emergency Vehicle Response/Vehicle Pursuit Operation	36.29.

36.1. Purpose. This chapter presents policy and guidance on the use of Defense Criminal Investigative Service (DCIS) motor vehicles. In addition, this chapter implements and supplements Inspector General Instruction (IGDINST) 4140.1, “Property Management Program,” January 3, 2007, Chapter 7, “Motor Vehicles.”

36.2. References

36.2.a. IGDINST 4140.1.

36.2.b. DoD Manual 4500.36, "Acquisition, Management, and Use of DoD Non-Tactical Vehicles," July 7, 2015.

36.2.c. IGDINST 4500.42, "Travel and Transportation Program," May 3, 2007.

36.2.d. Title 41, Code of Federal Regulations (CFR), Chapter 101, "Federal Property Management Regulations," July 1, 2011.

36.3. Authorization

36.3.a. Motor vehicle authorizations will be issued to field offices (FO) and resident agencies (RA), including posts of duty (POD) and Headquarters (HQ) directorates by the Deputy Inspector General for Investigations (DIG INV) based on individual office and agency-wide requirements.

36.3.b. Special Agents in Charge (SAC), Assistant Special Agents in Charge (ASAC), Resident Agents in Charge (RAC), and HQ Program Directors (PD) will continually ensure that the authorized size of their assigned vehicle fleet is appropriate for the number of employees and report any necessary reductions or increases to the DCIS HQ, Internal Operations Directorate, Policy and Internal Support (Internal Support).

36.4. Assignment. Continuous assignment of DCIS motor vehicles during normal duty hours is essential based on the responsibility inherent in criminal investigator positions and the fact that immediate availability of transportation is necessary to the accomplishment of the DCIS mission.

36.5. Acquisition. Acceptance of seized vehicles or vehicles from other Government agencies must be approved by the DIG INV. Requests for acceptance of these types of vehicles must be coordinated with the Department of Defense Inspector General (DoD IG), Office of General Counsel and submitted through Internal Support to the DIG INV.

36.6. Motor Vehicle Control Officers. Each SAC/ASAC/RAC/PD shall appoint, in writing, a Motor Vehicle Control Officer for each office location/directorate under their purview with assigned motor vehicles.

36.7. Authorized Drivers and Reporting Requirements

36.7.a. The SAC/ASAC/RAC/PD will ensure that only authorized personnel with valid licenses operate DCIS motor vehicles.

36.7.b. If at any time, a SAC/ASAC/RAC/PD becomes aware of any physical, medical, legal, or other condition that might adversely affect an employee's ability to operate a motor vehicle, the SAC/ASAC/RAC/PD will suspend that employee's privilege to operate a DCIS motor vehicle. The SAC/ASAC/RAC/PD may also recommend the employee for a medical examination,

depending on the circumstances. The DIG INV will make all final determinations for termination of an employee's privilege to operate a DCIS motor vehicle based on accident records, traffic violations, or the recommendation of medical officers.

36.7.c. Any employee that receives a citation for a traffic or parking violation occurring while operating a DCIS motor vehicle must report the citation or conviction to their immediate supervisor within 72 hours of the incident/action. This is not a substitute for any other reporting required for security clearance purposes.

36.7.d. Any employee whose state-issued motor vehicle license is suspended or revoked, whose driving privileges are restricted, or who otherwise becomes ineligible to operate a motor vehicle, must immediately report such action to their supervisor.

36.7.e. Any employee that is cited, arrested, or otherwise charged with driving under the influence (DUI) of drugs or alcohol or driving while intoxicated (DWI), regardless of whether the employee is driving a Government or privately owned vehicle, must immediately report such action to their supervisor.

36.7.f. If an armed DCIS agent is stopped by a law enforcement officer while operating a DCIS owned or leased vehicle, or any Government or privately owned vehicle, the agent will promptly inform the law enforcement officer of his or her status as a DCIS agent, and that he or she is armed, and display badge and credentials, in order to avoid a "blue-on-blue" incident. The DCIS agent will not make any statement or engage in any other behavior that could be construed as an attempt to avoid a traffic citation or other legitimate law enforcement action as a result of the agent's status. This requirement will not apply when the agent is engaged in officially authorized undercover activities as such actions could compromise those activities.

36.8. Motor Vehicle Identification

36.8.a. For reporting purposes, the Vehicle GSA, G-TAG, number will constitute the vehicle identification number (VIN). In addition, all DCIS vehicles will be entered into the Defense Property Accountability System (DPAS). The vehicles will be assigned to each property book holder at the FO/RA/POD where the vehicle is located. While this process will create a DIG number (a property accountability number in DPAS) for all vehicles, only the agency owned vehicles will use the DIG number as the VIN.

36.8.b. All DCIS motor vehicles are exempt from identification procedures as outlined in DoD 4500.36, Appendix 3 to Enclosure 5, "Guidance for Identification and Marking of Non-Tactical Vehicles."

36.9. Motor Vehicle Registration

36.9.a. Each vehicle, designated by the SAC/ASAC/RAC, will be properly registered in the state in which the office is located or in an adjoining state when necessary or advisable. (b)(7)(E)

(b)(7)(E)

(b)(7)(E)

36.9.b. GSA leased vehicles will be registered and inspected in accordance with instructions from the GSA Fleet Management Centers or Subcenters.

36.10. Official Use of Motor Vehicles

36.10.a. IGDINST 4140.1, Chapter 7, paragraph B.1., and DoD 4500.36-R, paragraph C2.5., require that the use of all DoD motor vehicles, including those leased from other Government agencies or commercial sources, shall be restricted to official purposes only (i.e., to further the mission of the agency). Questions as to whether an intended purpose is considered official use will be resolved in strict compliance with the above stated references and consideration will be given to all factors, including whether the use is:

36.10.a.(1). essential to the successful completion of a DCIS function, activity, or operation, and

36.10.a.(2). consistent with the purpose for which the motor vehicle was acquired.

36.10.b. The following official activities are considered use for official purposes:

36.10.b.(1). investigative, operational, technical, and administrative business;

36.10.b.(2). conferences and meetings; and

36.10.b.(3). training.

36.10.c. Additionally, DCIS motor vehicles can be used for transportation:

36.10.c.(1). by special agents (SAs) going to/from physical fitness training during duty hours and outside of duty hours if the SA is in a temporary duty (TDY) status, and

36.10.c.(2). to conduct official liaison activities. Liaison is defined as time spent meeting with Federal, state, and local agencies to encourage cooperation, enforcement of state laws, or the exchange of resources. In order to use a DCIS motor vehicle for transportation to an official liaison activity, the SA must be eligible to charge the liaison time on a DCIS Form 54, Biweekly Activity Report.

36.10.d. Use of a Government furnished vehicle is not permitted for conducting personal business or engaging in activities of a personal nature. Types of prohibited personal use include stopping at:

36.10.d.(1). eating establishments, unless this is done principally in support of an operational effort;

36.10.d.(2). shopping establishments of any kind;

36.10.d.(3). barber shops/beauty salons; and

36.10.d.(4). dry cleaning/laundry establishments.

36.10.d.(5) The only exception to this policy is addressed in IGDINST 4140.1, Chapter 7, paragraph C.6.e.(2). This paragraph states, “When an OIG owned or leased motor vehicle is authorized for use while on temporary duty, the vehicle shall be operated between places where the employee’s presence is required for official business, or between such places and temporary lodgings. When public transportation is not available or its use is impractical, the use of OIG owned or leased motor vehicles is authorized between places of business, lodging, eating establishments, drugstores, barber shops, places of worship, cleaning establishments, and similar places required for the comfort or health of the employee, and which foster the continued efficient performance of Government business...”

36.10.e. The unauthorized or willful misuse of a DCIS motor vehicle shall be cause for disciplinary actions as stated in IGDINST 4140.1, Chapter 7, paragraph B.2. If unauthorized or misuse of a Government-owned vehicle is substantiated, a 1-month suspension must be imposed. Additionally, financial liability shall be assessed against employees when a DCIS motor vehicle is lost, damaged, or destroyed as a result of the employee’s negligence, willful misconduct, or deliberate unauthorized use as stated in IGDINST 4140.1, Chapter 7, paragraph B.3. Administrative inquiries will be conducted in all instances of suspected unauthorized or willful misuse, and when motor vehicles are lost, damaged, or destroyed resulting from suspected negligence, willful misconduct, or deliberate unauthorized use.

36.11. Domicile-to-Duty (DTD) Transportation

36.11.a. In accordance with section 1344, title 31, United States Code (U.S.C.), 41 CFR 102-5, and DoD Regulation 4500.36, DoD motor vehicles are for official use only. Title 31 U.S.C. § 1344 and DoD 4500.36-R prohibit the use of an official vehicle for transport from an individual’s domicile to place of employment, commonly known as DTD, except as specifically depicted therein. Under 31 U.S.C. § 1344 and in accordance with DoD 4500.36-R, the Secretary of Defense may authorize, in writing, on a non-delegatable basis, DTD transportation. DTD will be approved only when it is considered essential for the safe and efficient performance of law enforcement duties. The approval is granted based on the criminal investigator position. The Internal Operations Directorate annually seeks DTD authorization from the Secretary of Defense and the current signed memorandum provides specific guidance on the implementation of this policy.

36.11.b. This authorization will be utilized on a case-by-case basis when it is “essential for the safe and efficient performance of...criminal law enforcement duties.” The comfort and convenience of an employee shall not be considered justification for the approval of DTD transportation. SACs, ASACs, RACs, and PDs shall act as the approving authority for SAs under their supervision. Based on the provisions of 41 CFR 102-5, DTD transportation shall only be authorized when such transportation substantially increases DoD efficiency and economy. In accordance with DoD 4500.36-R, DTD transportation will be provided only on days when the individual actually performs criminal law enforcement duties.

36.11.c. The SACs and PDs shall be responsible for monitoring the DTD transportation usage and compliance with applicable rules and regulations. Except for unusual circumstances, DTD transportation must be approved in advance and must be documented on DCIS Form 82, Domicile-to-Duty Log, (Attachment A). The entries on the Form 82 shall include:

36.11.c.(1). date DTD approved,

36.11.c.(2). SA's name,

36.11.c.(3). GOV number,

36.11.c.(4). location,

36.11.c.(5). duration of approval,

36.11.c.(6). justification necessitating DTD transportation, and

36.11.c.(7). name and title of person approving DTD transportation. The RAC or acting RAC is the approving authority for DTD.

36.11.d. The Form 82 is a management form, not an agent form. At the end of the month, the RAC will send the completed Form 82 to the FO where the SAC or ASAC will sign the document. This signature validates that the Form 82 is accurate and meets the regulatory criteria for DTD. The FO will post the Form 82 on the SharePoint site designated by Internal Support by the 7th business day of each month.

36.12. Carpooling. Carpooling will be authorized only with the express permission of the immediate supervisor. The operator of a Government furnished vehicle cannot deviate from the most direct, reasonable route and must not go to employees' residences to pick them up except when employees are departing directly from their residences to proceed together to a TDY location.

36.13. Passengers in Government Furnished Vehicles. Spouses, dependents, and other passengers that do not have official business are not permitted in a Government furnished or controlled vehicle.

36.14. Parking of Motor Vehicles. Vehicles will normally be parked in an approved secure area in proximity to DCIS offices. When domicile parking has been authorized, the employee shall ensure the vehicle's security to the maximum extent possible. Employees will provide the same level of care and security as that afforded to a personally owned vehicle.

36.15. Use of Government Furnished Vehicles in Lieu of Privately Owned Vehicles (POV). In accordance with requirements contained in DoD 4500.36-R, paragraph C2.8., Government furnished vehicles will be used for official business prior to voluntary use of POVs on a reimbursable basis, as long as Government furnished vehicles are available and capable of meeting mission requirements. Use of a POV for official business because an adequate Government furnished vehicle is not available must be authorized in writing by the SAC/ASAC/RAC/PD prior

to the use of the POV. When such use has been authorized, the employee is considered to be acting within the scope of their employment. Therefore, the employee is not personally liable in the event of an accident unless negligence or willful misconduct is determined. However, the employee could be held personally liable for loss of property and/or personal injury resulting from an accident in which they operated a POV without authorization and was, therefore, considered to be acting outside the scope of their employment.

36.16. Use of Commercially Rented Motor Vehicles

36.16.a. The use of commercially rented motor vehicles contracted for by DCIS employees for TDY purposes is addressed in IGDINST 4500.42, Chapter 3. The employee must identify himself/herself as a Government employee when renting the vehicle.

36.16.b. All requests for short-term leases (up to 60 days) for motor vehicles for operational purposes (other than TDY or specifically for transporting records related to investigative operations) must be forwarded by the SAC/ASAC/PD to the Deputy Assistant Inspector General for Investigations (DAIGI), Internal Operations. Penalties for misuse and financial liability as stated in IGDINST 4140.1, Chapter 7, paragraph B.3., also apply to the use of motor vehicles leased by the DoD IG. **Use of DCIS motor vehicles (GSA Integrated Fleet Management System (IFMS) vehicles and vehicles leased short-term for operational purposes) for other than official business is strictly prohibited.** When questions arise about the official use of a motor vehicle, they shall be resolved in favor of strict compliance with statutory provisions and DoD policy.

36.17. Use of Motor Vehicles by Non-DCIS Personnel

36.17.a. **Informants.** The use of DCIS motor vehicles by informants is prohibited except in a bona fide emergency.

36.17.b. **Other Law Enforcement Officers.** In accordance with IGDINST 4140.1, other law enforcement officers may operate DCIS motor vehicles when such use is in direct support of the DoD IG/DCIS mission and is approved by the SAC/ASAC/RAC/PD or used in a bona fide emergency situation without prior approval. All instances of emergency use without prior approval will be reported after the fact to the SAC/ASAC/RAC/PD.

36.17.c. **DoD IG Employees.** With DCIS supervisory approval, non-DCIS DoD IG employees are permitted to use DCIS motor vehicles for official business.

36.17.d. **Other Motor Vehicles.** DCIS SAs can operate another Federal agency's official motor vehicle within the guidelines of that particular agency. The SA should be familiar with the rules and regulations of that agency before driving the vehicle.

36.18. Theft and Vandalism

36.18.a. Employees will ensure that unattended DCIS motor vehicles and commercially rented vehicles are properly secured. Technical equipment and similar sensitive or costly equipment will not be stored in a vehicle. However, when use of the equipment is imminent, the

items may be kept in a locked trunk. Firearms, ammunition, badges and credentials, evidence, official funds, and other items of value shall not be placed in any unattended vehicle except as authorized in other SAM chapters. If circumstances dictate that it is prudent for a SA to temporarily store a DCIS-issued portable radio in an unattended vehicle, the radio should be concealed (out of sight) in the locked trunk of the vehicle. At no time will a DCIS-issued portable radio be stored overnight in an unattended vehicle.

36.18.b. Vandalism to and theft of or from a DCIS motor vehicle and theft from a commercially rented vehicle will be reported in the following manner.

36.18.b.(1). The operator will immediately notify the FO/Resident Agency (RA) and appropriate local law enforcement authorities.

36.18.b.(2). The FO/RA will notify Internal Support via e-mail within 24 hours using the notification form found on the DoD IG Intranet/Components/INV/Admin Toolbox/Vehicles(GOV/GSA)/Accident Reporting Procedures.

36.18.b.(3). The SAC/ASAC/RAC/PD will assign a SA to conduct the investigation. The investigating agent must be of equal or higher grade than the operator.

36.18.b.(4). The investigating agent will prepare a DD Form 200, "Financial Liability Investigation of Property Loss," for all damages/losses. Additionally, the investigating agent will prepare a detailed memorandum of the circumstances of:

36.18.b.(4).(a). all thefts of or from DCIS motor vehicles,

36.18.b.(4).(b). all damage from vandalism of DCIS motor vehicles, and

36.18.b.(4).(c). all thefts from commercially rented vehicles.

36.18.b.(4).(d). All required documents must be submitted to Internal Support by PDs within five (5) workdays and by SACs within ten (10) workdays.

36.18.b.(5). The vehicle operator will obtain three (3) estimates for repair (where applicable).

36.18.c. Internal Support and the SAC will maintain completed files on thefts and vandalism. Sufficient copies of each document will be furnished to supply these files.

36.19. Safety and Accident Prevention. Operators of DCIS motor vehicles shall wear a seat belt while operating a vehicle and ensure that all passengers fasten seat belts. Each DCIS motor vehicle will be equipped with at least the following items:

36.19.a. good spare tire (if provided by GSA) or tire inflator kit;

36.19.b. jack and lug wrench in good working condition (if provided by GSA);

36.19.c. dry-type fire extinguisher;

36.19.d. flares or triangle highway warning devices;

36.19.e. first-aid kit;

36.19.f. flashlight;

36.19.g. emergency equipment or materials necessary for the climate in which the vehicle is operated, (e.g., jumper cables, snow shovels, and tire chains in frigid climates, and emergency water in desert areas);

36.19.h. accident forms; and

36.19.i. bloodborne pathogens kits, these kits will be locally purchased. Direct all questions to Internal Support.

36.20. Alcohol and Drug Use

36.20.a. Under no circumstances shall the driver of a Government furnished vehicle operate the vehicle in an intoxicated condition or when alcohol, prescription drugs, or illicit drugs have made him/her an unsafe driver. SAs who have consumed alcohol may not operate a Government furnished vehicle until such time as the use of the vehicle would not be questioned due to the consumption of the intoxicant.

36.20.b. Except for rare and limited matters of operational necessity, such as certain undercover or surveillance activities, DCIS personnel are prohibited from consuming intoxicants and then driving a Government furnished vehicle. Employees who consume alcoholic beverages at events, such as Government agency officially sponsored conferences, meetings, liaison, and social functions, are prohibited from driving Government furnished vehicles. In such instances, making prior arrangements for an authorized designated driver is the prudent, responsible, and recommended course of action.

36.20.c. Employees that drive under the influence of illicit drugs or alcohol or that drive while intoxicated, whether established by a conviction in court or as the result of an internal administrative inquiry, are subject to disciplinary actions up to and including removal. This policy applies regardless of whether the employee is on- or off-duty, and whether driving a personally owned, commercially leased or rented vehicle, or a DCIS motor vehicle.

36.21. Motor Vehicle Accidents

36.21.a. All procedures outlined in IGDINST 4140.1, Chapter 7, paragraph H, will be followed regarding reporting of accidents involving DCIS motor vehicles and commercially rented motor vehicles. In all accident cases, the employee will immediately stop, render assistance to the injured, warn other motorists of any existing highway hazard, and obtain the names, addresses, and telephone numbers of other drivers involved and any witnesses. The employee will immediately notify their supervisor and local law enforcement authorities. All motor vehicle

accidents must be reported via e-mail within 24 hours of the accident. The forms required for completing the accident package are located on the DoD IG Intranet/Components/INV/Admin Toolbox/Vehicles(GOV/GSA)/Accident Reporting Procedures. All accidents involving DCIS motor vehicles, regardless of the dollar amount of the damage, will be investigated and documented on a DD Form 200 including the reporting of stolen, damaged, or destroyed vehicles. For any accident where the driver/operator was determined to be at fault, that driver/operator is required to complete the GSA Online Defensive Training Course, located at <http://www.gsa.gov/portal/content/102674>. The course will be completed within 30 days of the determination of fault, will be validated by the driver/operator's supervisor, and the completion certification will be forwarded to Internal Support.

36.21.b. Additionally, in accidents involving commercially rented motor vehicles, the employee operator will also complete the rental company accident form and provide it to the rental company.

36.21.b.(1). The employee must also forward the following, through their supervisors, to Internal Support:

36.21.b.(1).(a). a copy of the rental company accident form,

36.21.b.(1).(b). a copy of the rental agreement,

36.21.b.(1).(c). a copy of their travel orders, and

36.21.b.(1).(d). a statement describing the incident.

36.21.b.(2). Preparation of a DD Form 200 is not required for rental vehicles.

36.22. Investigation of Accidents/Theft/Vandalism

36.22.a. The SAC/ASAC/RAC/PD will assign a SA to conduct the investigation of all motor vehicle incidents. The SA assigned must be of equal or higher grade than the operator. Incidents will be documented in accordance with IGDINST 4140.1. The memorandum will include a determination concerning the cause of the incident and the surrounding circumstances, including how the incident could have been prevented. Additionally, three estimates for repair will be obtained (where applicable).

36.22.b. The investigating agent will ensure the following steps are completed.

36.22.b.(1). Fully complete, sign, date, and return all required forms and reports to the PD within three (3) workdays or the SAC within seven (7) workdays. PDs must submit final reports to Internal Support within five (5) workdays; SACs, within ten (10) workdays.

36.22.b.(2). Obtain photographs of the incident scene and damage to the vehicle and/or property.

36.22.b.(3). If personal injuries are involved, interview the appropriate physicians and, where possible, obtain written documentation of the injuries. If a death occurs, obtain a copy of the autopsy protocol and a death certificate.

36.22.b.(4). Prepare a supplemental memorandum when:

36.22.b.(4).(a). injury or death results but no written documentation could be obtained from the attending physician (report any oral remarks of the physician); and/or

36.22.b.(4).(b). a witness refuses to give a written statement but makes an oral statement as to cause or liability.

36.22.c. Completed files on vehicle incident investigations will be maintained by Internal Support and the SAC/PD.

36.23. Accident or Unsafe Practice Drug Testing

36.23.a. DoD IG is committed to providing a safe and secure working environment. It also has a legitimate interest in determining the cause of serious accidents so that it can undertake appropriate corrective measures. Accordingly, employees may be subject to drug testing when, based upon the circumstances of the accident, their actions are reasonably suspected of having caused or contributed to an accident that meets either of the following criteria.

36.23.a.(1). The accident results in a death or personal injury requiring immediate hospitalization.

36.23.a.(2). The accident results in damage to Government or private property estimated to be in excess of \$10,000.

36.23.b. If an employee's actions are suspected of having caused or contributed to an accident meeting either of the criteria stated above, the first-line supervisor will present the facts and circumstances leading to and supporting this suspicion to their supervisor for approval to request drug testing. Once approval has been obtained, the first-line supervisor will prepare a written request detailing the facts and circumstances that warrant the testing and provide it to the SAC/PD.

36.24. Claims

36.24.a. Claims for or against the Government will be processed by the regional Judge Advocate General's Office servicing the geographic area where the accident took place. Individuals involved in accidents with DCIS vehicles requesting information should be referred to Internal Support.

36.24.b. If insurance companies or claimants request a point of contact, refer them to Internal Support. Any written notices received should also be forwarded to Internal Support for inclusion in the accident report. DCIS employees are prohibited from expressing oral or written opinions to claimants or their agents concerning liability, investigation findings, or possibility of claim approval.

36.25. Maintenance, Repairs, and Services

36.25.a. **Maintenance.** The SAC/ASAC/RAC/PD will ensure that all DCIS motor vehicles are maintained and used uniformly. Vehicle use should be rotated to ensure annual mileage is approximately equal for all assigned vehicles necessary to ensure effective maintenance of the vehicles. Additionally, car windows should also be cleaned and window-washing fluids replaced frequently to ensure visual acuity. The GSA Commercial Fleet Services Card can be used for payment of these services. DCIS FOs and HQ should coordinate with the local GSA Fleet Center to ensure they are in compliance with the monetary guidelines for their area.

36.25.b. **Routine Maintenance.** Routine maintenance of GSA leased vehicles shall be accomplished in accordance with instructions from the servicing GSA Fleet Management Centers.

36.25.c. **Warranty Repairs and Services.** Repairs covered by the vehicle manufacturer's warranty must be promptly accomplished after the malfunction is detected. Undue delay may void the warranty and cause an unnecessary expenditure of funds.

36.25.d. **Non-warranty Repairs and Services.** Repairs and services for non-warranty items will be handled in the following manner. The GSA Commercial Fleet Services Card issued by GSA with each vehicle will be used only for those items listed on the back of the card, and the card will only be used for repairs and services to the vehicle for which it was issued. The Fleet Management Centers operated by GSA will authorize repairs and services over \$100.

36.25.e. **Emergency Repairs or Services.** For authorization of emergency repairs or services on GSA IFMS leased vehicles, employees should contact the appropriate GSA Fleet Management Center or Subcenter. When the employee is unable to reach the GSA Center for authorization, they may use the GSA Commercial Fleet Services Card; however, every attempt should be made to first contact GSA since DCIS may have to reimburse GSA for such charges over and above the agency's normal billing costs. The employee will contact GSA on the next workday to explain the circumstances for the emergency repairs and that he/she had tried, but was unable to reach GSA for prior authorization. GSA will bill DCIS for all repairs and services.

36.25.f. **Emergency and Extraordinary (E&E) Funds.** These funds will not be used for the repairs and services of any DCIS motor vehicle.

36.25.g. **Duplication of Repairs and Services Payments.** Accurate vehicle repair records and authorizations must be maintained by the Motor Vehicle Control Officers to avoid duplicate payment for any repairs or services.

36.25.h. **Unsatisfactory Repairs.** Employees that accept a repaired vehicle are responsible for ensuring that repairs are completed in a satisfactory manner. Unsatisfactory repairs will be reported to the local GSA representative and then the vehicle should be returned to the shop and the deficiencies corrected.

36.25.i. **Liability.** DCIS will not assume liability for any costs incurred by repair shops or vendors that undertake repairs or services of a vehicle without authorization from the employee that placed the vehicle in the custody of the shop or vendor. Caution will be exercised in selecting vendors to ensure that a reasonable warranty is provided for repair work that is performed.

36.26. Administrative Control of Credit Cards. Accountability of GSA Commercial Fleet Services Cards will be strictly maintained by each Motor Vehicle Operator to avoid loss and preclude the occurrence of unauthorized charges. The following specific administrative controls apply to these credit cards.

36.26.a. The Motor Vehicle Control Officer will promptly notify:

36.26.a.(1). the GSA Fleet Management Center or Subcenter for all lost or stolen GSA Commercial Fleet Services Cards, and

36.26.a.(2). Internal Support in writing of all lost or stolen GSA Commercial Fleet Services Cards, to include the date each card was discovered lost or stolen. Internal Support will promptly notify the Comptroller, DoD IG Mission Support Team, of all lost or stolen cards.

36.26.b. The following credit cards shall be promptly destroyed or returned to GSA when required:

36.26.b.(1). credit cards that have been replaced for any reason, to include lost or stolen credit cards recovered after having been reported lost or stolen;

36.26.b.(2). credit cards bearing an expiration date that has passed; or

36.26.b.(3) credit cards bearing an invalid license tag number, serial number, or other identifying number.

36.26.c. Invoices from credit card purchases shall be prepared legibly and completely at time of purchase, with signatures of operators being legible. Invoices should contain the VIN.

36.26.d. Supervisory personnel shall make periodic reviews to ensure that credit card safeguards are adequate, invoices are legible and reasonable compared to utilization records, and questionable transactions or practices are investigated immediately.

36.26.e. The SAC/PD via memorandum to the DAIGI Internal Operations will immediately report misuse of any Government credit card. The memorandum should include all the circumstances involving the reported misuse.

36.27. Cash Purchases in Lieu of Credit Cards. Cash purchases of gasoline and emergency repairs in lieu of credit card purchases will only be made in emergency situations, for example at a location where a vendor refuses to honor a Government credit card or in instances in which use of a Government credit card may compromise an investigation. Requests for reimbursement of emergency cash purchases will be processed in accordance with IGDINST 4500.42, Chapter 6.

36.28. Vehicle Management Reporting Procedures

36.28.a. The DCIS Form 10, DCIS Vehicle Log, dated September 2015, (Attachment B), is the **only** vehicle log authorized by DCIS for annotating vehicle mileage and usage data. No locally designed or produced forms are allowed. The Form 82 (Attachment A) is the authorizing document for the DTD entries contained in the DCIS Form 10. These two documents represent the cornerstone of the DCIS vehicle management program.

36.28.b. The Form 10, as well as the Form 82, and all supporting documents will continue to be reported and uploaded by the 7th business day of each month to the Internal Support, SharePoint site. The supporting documentation includes all fuel (GSA requires only unleaded fuel purchases), maintenance, and any other documents or receipts related to the vehicle for the reporting month. In addition, when a vehicle is returned to GSA for any reason, the turn-in documentation will be uploaded as part of the vehicle's supporting documents for the last month of use. When any new or replacement vehicles are received from GSA, the gaining documents will be uploaded with the vehicle's Form 10 documentation for the first month of use. The requirement to enter mileage data into the GSA Mileage Express remains in effect and is the responsibility of the FO, RA, POD, or HQ directorate.

36.28.c. Implementing Instructions for Form 10 are listed below. In order to support DCIS' Vehicle Allocation Methodology, it is crucial that all data be accurate and timely.

36.28.c.(1). Administrative Data

36.28.c.(1).(a). Monthly Mileage. Odometer Reading on the first day of the month will be entered next to Begin, and the odometer reading on the last day of the month will be entered next to End. Subtract the Begin mileage from the End mileage and enter next to Total.

36.28.c.(1).(b). G-Tag. Enter the GSA vehicle number in this block (e.g. G12-1234M).

36.28.c.(1).(c). GOV Description. Enter the make, model, year, and color of the vehicle.

36.28.c.(1).(d). Office. Enter the FO, RA, POD, or HQ directorate where the vehicle is located (e.g. 10BN).

36.28.c.(1).(e) Month/Year. Enter the month and year the Vehicle Log covers (e.g. July 2015).

36.28.c.(1).(f). Total DTD Used. Enter the number of DTD days by adding the number of X's listed under the DTD Used column.

36.28.c.(1).(g). Total Trips. Enter the number of trips by adding the trip numbers listed in the Trips column.

36.28.c.(2). **Vehicle Activity Data**

36.28.c.(2).(a). Date. Enter the day of the month that the vehicle was driven (e.g. 3/17/2015).

36.28.c.(2).(b). Activity Code. Enter a code using the Usage Code Key legend at the bottom of the Form 10. Each code represents a destination. Separate the destination codes by a comma. Choose the appropriate code from the key. If no code represents the destination, use the "other code" and briefly describe the activity. If there are more destinations than can be entered on one line under Activity Code, then continue on the line below.

36.28.c.(2).(c). DTD Used. Enter an X for each day of the month when the vehicle is located at the driver's residence following the end of that duty day. DTD must be approved on the DCIS Form 82 for the day/days the vehicle is located at the residence. TDY does not fall under DTD. The TDY orders authorize the vehicle to be parked at a location that is not the duty location.

36.28.c.(2).(d). Trips. Enter the number of trips as defined by the number of destinations to which a GOV is driven on any given day. For example, if a driver leaves from their residence, travels to execute a search warrant (1), then to the office (2), then to brief the AUSA (3), then to interview a witness (4), and then back to the office to park the GOV for the day (5), that constitutes 5 trips for that day.

36.28.c.(2).(e). Driver. Enter the legible name for the driver of the vehicle for each day driven.

36.29. Emergency Vehicle Response/Vehicle Pursuit Operation

36.29.a. **Purpose**. The purpose of this section is to establish a uniform emergency vehicle response policy.

36.29.b. **Authority**. The authority of the DIG INV to issue this directive is derived from 10 U.S.C. § 1585a.

36.29.c. Definitions

36.29.c.(1). **Emergency Vehicle Response**. The method and manner in which a DCIS SA operates an authorized emergency vehicle when responding to a situation in which a DCIS SA or other individual is in imminent danger of serious bodily injury or death.

36.29.c.(2). **Vehicle Pursuit.** The method and manner in which a DCIS SA operating an authorized emergency vehicle follows another vehicle for the purpose of stopping and apprehending an occupant(s) of that other vehicle, when the occupant(s) of that vehicle is attempting to avoid apprehension by maintaining or increasing the speed of said vehicle, or by ignoring the DCIS SA's attempt to stop such vehicle.

36.29.c.(3). **Authorized Emergency Vehicle.** A Government-owned or leased vehicle equipped with operable emergency equipment, including audible siren and appropriately colored flashing or stationary warning lights, while a DCIS SA is operating such vehicle.

36.29.c.(4). **Roadblock.** A restriction or obstruction used or intended for the purpose of preventing free passage of motor vehicles on a roadway.

36.29.c.(5). **Appropriate Emergency Equipment.** Emergency lights that shall be red, blue, or other color designated by state or local statute, flashing or stationary, and are visible, under normal atmospheric conditions, from a minimum distance of 1,000 feet for 360 degrees around the vehicle. The vehicle will also be equipped with a siren system with a minimum 100-watt siren speaker and have wail and yelp siren modes available. The emergency equipment should meet or exceed the statutory requirements of the state or jurisdiction where the DCIS SA's office is located or where the vehicle is to be operated.

36.29.c.(6). **State Motor Vehicle Regulations.** Those regulations put into place by a state or political subdivision that govern the safe operation of a motor vehicle by the general motoring public. **This does not include those regulations that allow for the emergency operation of state and local law enforcement vehicles for emergency purposes.**

36.29.d. **Policy**

36.29.d.(1). Emergency response and vehicle pursuit activities will only be undertaken with authorized emergency vehicles.

36.29.d.(2). Operating an authorized emergency vehicle in an emergency response scenario presents a significant danger to the lives and property of the general public, as well as the lives of those DCIS SAs involved. Every DCIS SA must understand that the use of emergency equipment when engaging in an emergency response is merely a ***request for the right-of-way*** by an emergency vehicle, and does not guarantee that right-of-way. The fact that a DCIS SA is engaged in an emergency response does not relieve the DCIS SA from the duty to operate the authorized emergency vehicle with due regard for the safety of all persons using the roadway, nor protect that DCIS SA from the consequences of an arbitrary exercise of the privileges accorded to an emergency vehicle under state law.

36.29.d.(3). A vehicle pursuit scenario represents a significant danger to the lives and property of the general public, and the lives of DCIS SAs and occupant(s) of the vehicle being pursued. Accordingly, under no circumstances shall a DCIS SA operate an authorized emergency vehicle during a vehicle pursuit in a manner inconsistent with the state motor vehicle regulations governing the geographic location where a vehicle pursuit occurs.

36.29.d.(4). No DCIS SA will use a DCIS motor vehicle, including but not limited to an authorized emergency vehicle, to construct a roadblock.

36.29.d.(5). No DCIS SA will engage in an emergency vehicle response or vehicle pursuit while transporting prisoners, witnesses, suspects, or any other non-law enforcement personnel in the authorized emergency vehicle.

36.29.d.(6). SACs will identify/certify on an annual basis those Government-owned vehicles under their cognizance that are authorized emergency vehicles. These certifications shall be maintained at each FO and available for inspection upon request. Additionally, a copy of the certification shall be provided to each SA under the SAC's cognizance.

ATTACHMENTS

A DCIS Form 82, "Domicile-to-Duty Authorization Log," dated May 2008

B DCIS Form 10, "Vehicle Log," dated September 2015

ATTACHMENT A

DCIS FORM 82, DOMICILE-TO-DUTY AUTHORIZATION LOG

DOMICILE-TO-DUTY AUTHORIZATION LOG						Office:
						Month:
Date	Special Agent	GOV #	Location	Duration	Justification	Approving Authority/Title

RAC Review _____ ASAC/SAC Review _____
Date/Initials Date/Initials

DCIS 82, MAY 2008

ATTACHMENT B

DCIS VEHICLE LOG

[illegible]

Activity Code Key:

A = Residence

B = Duty Station

C = TDY (Meal/Hotel/Work Location/Other)

D = Surveillance

E = Search/Arrest Warrant

F = Conduct Interview(s)

G = Other LE Operational Activity (e.g., subpoena service, trash cover)

H = Meeting(s)

I = Briefing/Liaison

J = Training (*Physical Fitness/Firearms/Other*)

K = Fuel/Maintenance/Carwash

L = Other (describe "other" activity)

NOTE: Provide all receipts for fuel, maintenance, and any fleet card-related charges with the Form 10 at the end of each month.



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

April 29, 2016

MEMORANDUM FOR ALL DCIS SPECIAL AGENTS

SUBJECT: Interim Policy for Special Agents Manual (SAM) Chapter 36, "Motor Vehicles,"
regarding DCIS Domicile to Duty Guidelines

Effective May 1, 2016, this interim policy rescinds paragraph 36.10.c.(1)., revises paragraph 36.10.d., and revises paragraph 36.11.a. of SAM Chapter 36. This policy provides guidance on the updated DCIS Domicile to Duty (DTD) Program.

Implementing Instructions. The following provides the policy guidelines for the DCIS DTD Program.

36.10. Official Use of Motor Vehicles. The language contained in paragraph 36.10.c.(1). is hereby rescinded. Paragraph 36.10.d. is revised to state:

In accordance with DoD Manual 4500.36, "Acquisition, Management, and Use of DoD Non-Tactical Vehicles," Enclosure 5, paragraph 1.b., each DoD Component head, or designee, may prescribe by rule appropriate conditions for the incidental use for other than "official" business of U.S. Government-owned or Government-leased Non Tactical Vehicles (NTVs), pursuant to title 31, United States Code, Section 1344, "Passenger carrier use." Except for minor incidental personal use, DCIS vehicles shall not be used for personal matters, recreation, or personal transportation. However, minor incidental personal use such as a brief stop normally not to exceed 15 minutes while on direct route between duty assignments or during DTD travel is authorized. Use of a DCIS vehicle by agents going to/from physical fitness training during duty hours and outside of duty hours is authorized. Use of a DCIS vehicle by agents is also authorized for going on a meal break from the office or site of official business when adequate eating facilities are not located within or in reasonable walking distance of the building.

36.11. Domicile to Duty Transportation. Paragraph 36.11.a. is revised to state:

In accordance with title 31, United States Code, Section 1344, "Passenger carrier use," the Acting Inspector General requested that the Secretary of Defense authorize full-time, blanket DTD transportation to DCIS GS-1811 Criminal Investigators (agents). Consistent with Section 1344(a)(2) of this statute, the transportation between the residence of the agent and various locations is "essential for the safe and efficient performance of ... criminal law enforcement duties." On April 29, 2016, the Secretary of Defense signed a memorandum that empowered the Acting Inspector General to make the decision regarding DTD transportation by issuing guidance and direction to supervisory personnel within DCIS, who based on such guidance and direction can determine which specific DCIS agents under their supervision and control are authorized DTD on a blanket or continuous basis. On April 29, 2016, the

~~FOR OFFICIAL USE ONLY~~

Acting Inspector General authorized full-time, blanket DTD transportation for agents actively conducting criminal investigations and their first line supervisors. The Acting Inspector General has determined that full-time, blanket DTD authority will enhance the safety, efficiency, and effectiveness of agents. While conducting and directly supervising criminal investigations, agents must be available at a moment's notice to respond to unanticipated critical investigative activity. Having access to a law enforcement vehicle at all times, properly equipped, and with their equipment and safety gear always available to them, enables them to do so safely and efficiently. Special Agents in Charge (SACs), Assistant Special Agents in Charge (ASACs), or any agents assigned to a Headquarters criminal investigator position will only have DTD transportation on a case-by-case basis. The DCIS Form 82, "Domicile-to-Duty Authorization Log," will no longer be required for agents in the field or first line supervisors. However, the current policy as stated in paragraph 36.11.c. and 36.11.d. related to DTD and the Form 82 will continue for SACs, ASACs and Headquarters agents.

Management Internal Control Requirements. In accordance with DoD Manual 4500.36, the following DTD internal controls will be incorporated into SAM Chapter 36.

- A. The DCIS Form 10, "DCIS Vehicle Log," will continue to be completed by all agents and vehicle drivers and posted per instructions in SAM Chapter 36, paragraph 36.28.
- B. The DCIS Form 82 for DTD authorizations related to SACs, ASACs, and Headquarters' agents will be posted per instructions in SAM Chapter 36, paragraph 36.11.d.
- C. The SACs are responsible for conducting an annual audit of driver qualifications.
- D. The SACs are responsible for ensuring all agents within their respective Field Offices receive instruction on the proper use of DoD NTVs, which includes all DCIS leased or owned vehicles, along with recurring and new user training on DTD limitations as stated in the revised SAM Chapter 36.

This policy is in effect until it is rescinded or incorporated into the next revision of SAM Chapter 36. Any questions related to this policy should be directed to me at (703) 604-6, (b)(7)

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

Deputy Assistant Inspector General
for Investigations

CHAPTER 38

USE OF FORCE

<u>Contents</u>	<u>Section</u>
General	38.1.
Definitions	38.2.
Use of Force Policy	38.3.
Use of Force	38.4.
Use of Force While in a Deployed Status	38.5.
Use of Force While Operating in Foreign Countries	38.6.
Use of Force Involving Non-Federal Crimes	38.7.
Use of Force Incident Management	38.8.
Rights of Special Agents Involved in Use of Force Incidents	38.9.
Use of Force Reporting Requirements	38.10.
Reporting Requirements Involving Prohibited Activities	38.11.
Use of Force Equipment	38.12.
Control Tactics Instructors	38.13.
Control Tactics Training	38.14.
Firearms Authority	38.15.
Firearms Policy	38.16.
Firearms Standards	38.17.
Firearms Security/Safety	38.18.
Ammunition Standards	38.19.
Holster Standards	38.20.
Firearms Instructors	38.21.
Firearms Training	38.22.
Firearms Maintenance	38.23.

38.1. General. This chapter contains policies and procedures pertaining to the Use of Force Program for all DCIS special agents/criminal investigators. Unless otherwise noted, all references to “DCIS special agents” and/or “DCIS instructor cadre” apply to the aforementioned special agents/criminal investigators. This policy is in accordance with the following references.

38.1.a. Title 10, United States Code (U.S.C.), section 1585, “Carrying of Firearms” (by civilian officers and employees of the Department of Defense).

38.1.b. Title 10, U.S.C., section 1585a, “Special agents of the Defense Criminal Investigative Service: authority to execute warrants and make arrests.”

38.1.c. Title 18, U.S.C., section 922(g) (8) and (9), also known as the Domestic Violence Amendment to the Gun Control Act of 1968 and the Lautenberg Amendment to the Gun Control Act of 1968.

38.1.d. Title 28, U.S.C., section 2671(105 Pub. L. 277, Title IV, Section 627(b), also known as the Federal Law Enforcement Officers’ Good Samaritan Act.

38.1.e. DoD Directive 5210.56, “Carrying of Firearms and the Use of Force by DoD Personnel Engaged in Security, Law and Order, or Counterintelligence Activities,” April 1, 2011.

38.1.f. DCIS Special Agents Manual (SAM) Chapter 1.6.d., “Arrest Authority,” August 2014

38.1.g. Title 5, U.S.C., sections 8401(17) and 8331(20), “Government Organization and Employees” (Federal law enforcement officer defined).

38.1.h. DoD Instruction 5100.76, “Safeguarding Conventional Arms, Ammunition, and Explosives (AA&E),” February 28, 2014.

38.1.i. Inspector General Instruction 4140.1, “Property Management Program,” January 3, 2007.

38.1.j. Inspector General Instruction 5210.56, “Carrying of Firearms by OIG Personnel,” November 4, 2004.

38.1.k. DoD Instruction 5525.12, “Implementation of the Amended Law Enforcement Officers Safety Act of 2004 (LEOSA),” February 13, 2014.

38.1.l. *Graham v. Connor*, 490 U.S. 386 (1989), which holds that during an arrest, investigatory stop, or other seizure, law enforcement officials will be held to an objective reasonableness standard in the use of force.

38.1.m DoD Instruction 5106.01, “Inspector General of the Department of Defense,” April 20, 2012.

38.2. Definitions

38.2.a. **Use of Force.** Use of Force is a degree of physical coercion or threat to effect an arrest, investigative stop, or seizure.

38.2.b. **Level of Force.** Level of force refers to the degree of force deemed objectively reasonable for the special agent to utilize, in light of the facts and circumstances confronting the special agent, to lawfully control an individual or situation or to otherwise accomplish a law enforcement purpose.

38.2.c. **Deadly Force.** Deadly force is any force likely to cause death or serious physical injury. This does not include the use of less-lethal force that, when used unexpectedly, results in death or serious physical injury.

38.2.d. **Less-Lethal Force.** Less-lethal force is the level or degree of force that is less likely or not intended to cause death or serious physical injury.

38.2.e. **Serious Bodily Injury or Physical Injury.** Serious bodily injury or serious physical injury means bodily injury that involves a substantial risk of death, extreme physical pain, protracted and obvious disfigurement, or protracted loss or impairment of function of a bodily member, organ, or mental faculty.

38.2.f. **Control.** Control refers to the use of force by a special agent to subdue a subject, effect an arrest, or otherwise accomplish a law enforcement purpose.

38.2.g. **Impact Weapon.** An impact weapon is any device that can be used as a weapon capable of transferring kinetic energy to a subject upon impact through a strike. DCIS defines an expandable baton as an impact weapon.

38.2.h. **Control Tactics.** Control tactics refer to techniques and methods designed to assist the special agent in overcoming levels of resistance.

38.2.i. **Special Agents in Charge.** For the purposes of this policy, any reference to the Special Agent in Charge (SAC) will include Field Office SAC (SAC, FO) and DCIS Headquarters (HQ) Deputy Assistant Inspectors General (DAIGs)—DAIG for Investigative Operations (DAIG, INV), DAIG for International Operations (DAIG, INTL), and DAIG for Internal Operations (DAIG, INT).

38.2.j. **Use of Force Program Manager.** The Use of Force Program Manager (UoF PM) is the individual designated as the national administrative coordinator for the DCIS Control Tactics and Firearms Programs. The UoF PM will provide administrative assistance to field coordinators.

38.2.k. **Field Office Firearms Coordinator (FOFC)/Field Office Control Tactics Coordinator (FOCT).** The coordinator is a special agent designated by the SAC, FO or HQ DAIG to administer the overall Control Tactics or Firearms Programs for an office. Coordinators will be certified instructors through the Federal Law Enforcement Training Center (FLETC) for their respective disciplines. Each field office and HQ will assign a special agent as a FOFC and a FOCT. These special agents will be the primary contacts with the UoF PM.

38.2.l. **Instructor.** The instructor is a special agent who has been trained and certified by FLETC to provide either Control Tactics and/or Firearms training.

38.2.m. **Training Materials.** The DCIS UoF PM has compiled an extensive collection of training materials concerning use of force, control tactics, officer safety, legal issues, and firearms. These materials include, lesson plans, courses of fire, and other relevant training aids. The materials are stored on the DCIS HQ network shared drive at S:\DCIS\Use of Force Program in related subfolders.

38.2.n. **Reporting Procedures.** Completing certain reports is necessary to comply with requirements in this chapter. Examples of these reports are attached for informational purposes. Reporting requirements may be met by either hard-copy memorandum or by electronic transmission.

38.2.o. **DCIS Use of Force Database (UFDB).** Training records and equipment are tracked through the use of forms, memoranda, and electronic spreadsheets. Use of Force and Firearms training results are captured on a “Use of Force Training Data” form, DCIS Form 52. The collective FY summary results are then recorded in a password-protected spreadsheet by field office or HQ and maintained centrally on the shared drive, at S:\DCIS\Use of Force Program. Original Forms 52 are maintained at the field level by the requisite instructors. In addition, a new centralized repository in the form of an electronic database is being developed to capture Use of Force training records by individual and to track agency-issued equipment by individual.

38.2.p. **DCIS Firearms Inventory Control Manager (FICM).** The DCIS special agent assigned to maintain the DCIS weapons inventory.

38.2.q. **DCIS Use of Force Program Coordinator (UoF PC).** The DCIS special agent who may serve as the FICM and directly supports the UoF PM.

38.2.r. **Long Guns.** Government-issued rifles and shotguns.

38.2.s. **Special Agent.** Criminal investigators (GS-1811) of the Department of Defense, Office of Inspector General (DoD IG), DCIS.

38.3. Use of Force Policy

38.3.a. **General.** The primary consideration for the use of force is the timely and effective application of the reasonable level of force necessary to lawfully control an individual or situation. Paramount considerations are preserving life and preventing physical injury. The reasonableness of a special agent’s use of force is governed by whether the special agent’s actions are objectively reasonable in light of the facts and circumstances confronting the special agent at the time of the incident, without the benefit of hindsight. Any determination of reasonableness must take into account the fact that special agents are often forced to make split- second decisions—in circumstances that are tense, uncertain, and rapidly evolving—about the level of force necessary for a particular situation. Accordingly, all situations will be resolved using that amount of force deemed objectively reasonable by a special agent, under the totality of circumstances, in accordance with DCIS Use of Force training, which is consistent with legal precedents set forth in *Graham v. Connor*, 490 U.S. 386 (1989).

38.3.b. **Reasonable Force.** A special agent may use the level of force he or she perceives objectively reasonable to accomplish the law enforcement purpose, taking into account the objectively reasonable perception of the totality of circumstances, including the escalation/de-escalation of resistance and other acts of the subject. The levels of force are intended to be fluid and are not rigid processes requiring a systematic approach before proceeding or receding to another level of force.

38.4. Use of Force

38.4.a. Use of Force Incident. A use of force incident is any use of force in pursuit of a law enforcement objective (e.g., discharge of a DCIS issued or authorized personally owned firearm, deployment of an intermediate weapon, weaponless control techniques, physical force, etc.) by a DCIS special agent or by any officer or agent of another agency during a joint investigation.

38.4.b. Less-Lethal Force. A special agent will use less-lethal force if it is reasonable to lawfully control an individual or situation, or to accomplish the law enforcement purpose.

38.4.c. Deadly Force. A special agent is authorized to use deadly force only when one or more of the following conditions exist.

38.4.c.(1). Self-Defense. A special agent is faced with an immediate threat of death or serious physical injury, and the use of deadly force is objectively reasonable for self-protection.

38.4.c.(2). In Defense of Another. A third party is faced with an immediate threat of death or serious physical injury, and the use of deadly force is deemed objectively reasonable to protect the third party from that immediate threat of death or serious physical injury.

38.4.c.(3). Fleeing Persons. Firing at fleeing persons is prohibited, unless that fleeing person poses a threat of death or serious physical injury to the special agent or to a third party, and the use of force is deemed objectively reasonable to protect either the special agent or the third party from the threat of death or serious physical injury.

38.4.d. Verbal Warning. A verbal warning to submit to the authority of the special agent should be given before using deadly force, but only if feasible and if doing so would not endanger a special agent or other person.

38.4.e. Warning Shots. Warning shots are prohibited.

38.4.f. Vehicles. Firing at a moving vehicle is prohibited except under the following circumstances: when the vehicle is being used as a weapon and poses a threat of death or serious physical injury to the special agent or others; or when the operator or occupant of a vehicle poses a threat of death or serious physical injury to the special agent or to others.

38.4.g. Animals. Force may be used against vicious dogs or other animals in self-defense or in the defense of others.

38.5. Use of Force While in a Deployed Status. While deployed to support an overseas contingency operation, the DCIS Use of Force Policy shall apply to incidents in furtherance of the special agent's law enforcement duties, unless otherwise stated in the Status of Forces Agreement. However, the DCIS Use of Force Policy shall not apply to the special agent's response to combat-related incidents where Standing Rules of Engagement are designated by Executive Order, Public Law, or DoD certification.

38.6. Use of Force While Operating in Foreign Countries. While operating in foreign countries, special agents will adhere to the DCIS Use of Force Policy guidance mandated by the Department of State, and/or the Status of Forces Agreement and/or Bilateral Security Agreement (where applicable). This provision does not apply to special agents deployed to support an overseas contingency operation, as noted in section 38.5.

38.7. Use of Force Involving Non-Federal Crimes. No specific Federal statute or regulation authorizes a special agent to intervene in non-Federal criminal matters. Therefore, in the absence of a specific statute conferring some special status upon a Federal law enforcement officer, a special agent who intervenes in a non-Federal criminal situation does so solely in his/her capacity as a private citizen. Public Law 105-277, Title IV, section 627(b), October 21, 1998, provides that under certain circumstances, a Federal law enforcement officer, for the purposes of tort liability, will be construed as acting within the scope of employment if the officer “takes reasonable action, including the use of force, 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 is threatened with bodily harm; or (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.”

38.8. Use of Force Incident Management. Special agents should apply the following procedures when serious injury, property damage, or death results from the use of force. These procedures are intended as guidelines; they are not intended to be all-inclusive or limiting.

38.8.a. Special agents should:

38.8.a.(1). place the subject under arrest (if appropriate) and secure the scene;

38.8.a.(2). notify and request local law enforcement response (sole Federal jurisdiction will require FBI notification and response);

38.8.a.(3). seek emergency medical treatment for those persons injured and render first aid when reasonable;

38.8.a.(4). maintain a secure scene pending response for crime-scene processing;

38.8.a.(5). notify their immediate supervisor as further detailed in 38.10; and

38.8.a.(6). relinquish firearms, if discharged, to local law enforcement authorities or FBI for crime- scene processing. It is recommended the weapon(s) be released to another DCIS special agent or DCIS supervisor as opposed to directly releasing the weapon(s) to the responding crime-scene personnel.

38.8.b. Supervisors should:

38.8.b.(1). oversee protection of subject(s), witness(es), other special agents, and the evidence;

38.8.b.(2) act as an intermediary or assign a “companion agent” to act as an intermediary between the special agent(s), and local law enforcement/FBI; and

38.8.b.(3). ensure that the special agent(s) involved in the incident receive prompt medical attention, if needed, are removed from the scene as soon as possible, and are not subject to media attention;

38.8.b.(4). If a special agent(s) is injured, the supervisor should designate someone who knows the family, a senior special agent, or a first-line supervisor to make personal contact with the agent’s family and offer transportation to the site of treatment, if it is in the local commuting area.

38.9. Rights of Special Agents Involved in Use of Force Incidents. Special agents involved in a use of force incident are entitled to immediate medical treatment. Personnel involved in a use of force incident will be allotted at least two sleep cycles before providing a formal statement pertaining to the incident.

38.9.a. **Legal Representation:** In the event a use of force incident results in serious injury or death, the special agent involved may become the target of local, state, or Federal criminal investigations. The special agent(s) has the right to consult with an attorney of his or her choosing before being questioned by investigators. In addition, emergency interim legal representation **may** be available from private counsel at Government expense, in accordance with the Attorney General’s guidelines on Legal Representation in Critical Incidents. Attachment A outlines the procedure for obtaining this assistance.

38.10. Use of Force Reporting Requirements: A DCIS special agent shall immediately report, as soon as practical, any use of force incident, to his or her first-line supervisor. The supervisor through the appropriate chain of command shall promptly notify the DAIG-INT and the Assistant Inspector General for Investigations for Investigative Operations (AIGI- INV). Those use of force incidents that result in death, serious injury, or property damage will immediately be reported by the AIGI-INV to the Office of General Counsel (OGC) and the Assistant Inspector General, Office of Quality Assurance and Standards (AIG-QAS) or the QAS Director of Investigations, as referenced in QAS Policy Manual, Chapter 2, “Investigations,” section 2.3.n. DCIS SAM Chapter 51, “Critical Incident Management,” shall be followed should a critical incident, as defined in SAM Chapter 51, occur. Special agents who sustain injury as a result of a use of force encounter must report this injury on an Office of Workers’ Compensation Program (OWCP) Form CA-1 to their supervisor through HCAS.

38.11. Reporting Requirements Involving Prohibited Activities. Any incident of a prohibited firearms activity (noted in paragraph 38.16.b.) involving a DCIS issued or authorized personally owned firearm, by any DCIS employee, must immediately be reported to the employee’s first-line supervisor. The supervisor through the appropriate chain of command shall promptly notify the DAIG, INT and the AIGI-INV. The AIGI-INV shall immediately notify the OGC and AIG-QAS or the QAS Director of Investigations, as referenced in QAS Policy Manual, Chapter 2, “Investigations,” section 2.3.n.

38.12. Use of Force Equipment

38.12.a. **Background.** DCIS provides special agents law enforcement equipment and training to assist them in safe and efficient mission execution. (b)(7)(E), (b)(7)(F)

(b)(7)(E), (b)(7)(F)

38.12.b. **Uniforms/Personal Protective Equipment.** Subject to availability of funding, DCIS will procure and equip OIG personnel with uniforms and personal protective equipment (PPE) when operationally required, adhering to DoDI 1400.25, Volume 591, “DoD Civilian Personnel Management System: Uniform Allowance Rates for DoD Civilian Employees,” March 12, 2009. The purpose of uniforms/PPE is to provide identification of law enforcement personnel and to protect special agents from physical hazards and bloodborne pathogens they may encounter in their official duties. DCIS will provide PPE in accordance with 5 U.S.C. 7903, “Protective Clothing and Equipment.” Wearing personal protective equipment and uniforms is authorized during search warrants, arrest warrants, specialized surveillance operations, rescue and recovery operations, control tactics and weapons training, deployments to high-risk environments, special enforcement operations, and other circumstances that may warrant it. To enhance safety during training, the instructor cadre will wear DCIS-issued garments identifying them as instructors. Permanent staff assigned to the DCIS Training Division will wear instructor designated clothing/PPE while performing instructional duties.

38.12.b.(1). Uniforms requested are grouped in the following categories:

38.12.b.(1).(a). CAT I: Special Agents—continental United States/outside the continental United States (CONUS/OCONUS) (permissive environments);

38.12.b.(1).(b). CAT II: Special Agents—OCONUS (non-permissive environments);

38.12.b.(1).(c). CAT III: Field Instructors—(Firearms/Control Tactics/Health & Wellness);

38.12.b.(1).(d). CAT IV: FLETC Instructor Cadre;

38.12.b.(1).(e). CAT V: FLETC Adjunct Instructors;

38.12.b.(1).(f). CAT VI: Special agents participating in DCIS-specific training aboard FLETC.

38.12.b.(2). The components of each category are denoted in Attachment B and have been validated based on mission need and safety protocols.

38.12.c. **Individual Use of Force Equipment.** All DCIS special agents will be issued the DCIS Basic Agent Gear (BAG), the contents of which are noted on DCIS Form 83, “DCIS Use of Force and Protective Equipment Hand Receipt,” (Attachment C). The BAG kit is intended for personnel operating within CONUS on non-expeditionary missions. DCIS personnel deploying to OCONUS non-permissive expeditionary environments will be issued the DCIS Individual Deployment Equipment (IDQ). The contents of the IDQ are noted on Attachment D, which serves as the hand receipt. Personal protective body armor will be issued to agents as soon as possible after they are hired by DCIS. The date of issue will be recorded by the UoF PM or UoF PC. Many body armor manufacturers currently offer a 5-year warranty on the vest inserts. Though the National Institute of Justice recognizes that body armor can last well beyond 5 years if properly maintained, many criminal justice agencies have adopted a 5-year armor-replacement cycle to stay within the manufacturer’s warranty. Subject to availability of funding, each agent’s armor will be collected and replaced within 48-72 months of the initial issue date. Personal protective body armor should be worn in the manner for which it was designed, tested, certified, and prescribed by the manufacturer. Each agent is responsible for following the specific use, wear, and care instructions provided by the manufacturer in the owner’s manual supplied with the vest.

38.12.d. **Use of Force Equipment for Field Elements.** Each field element (FO, RA, POD, FLETC) will have varying operational requirements dictating the need for use of force equipment (b)(7)(E), (b)(7)(F) Field Office Firearms Coordinators and Field Office Control Tactics Coordinators, with supervisory endorsement, will draft requests for specific equipment for processing by the Use of Force Program Coordinator (UoF PC). Final approval of requests will reside with the DAIG, INT, or their delegate. Budgetary control and validated mission requirements will dictate actual issuance of equipment. When applicable, adhere to the property management protocols in IGDINST 4140.1, “Property Management Program.”

38.12.e. **Accountability.** Special agents are responsible for the accountability and maintenance of agency-issued use of force–related equipment. The UoF PC will manage issuance of uniforms/protective clothing and equipment (excluding FLETC student uniforms and deployment uniforms) and will document via DCIS Form 83, “DCIS Use of Force and Protective Equipment Hand Receipt” (Attachment C). Completed Forms 83 will be maintained by the local control tactics instructor. A copy of the completed forms *must* be forwarded to the UoF PC. Uniforms and/or equipment that are non-serviceable or lost (excluding firearms) shall be validated by the first-line supervisor. Any request for replacement gear must be made from the first-line supervisor via an e-mail request to the UoF PC. Budgetary control and validated mission requirements will dictate actual replacement of equipment. All uniforms and equipment are DCIS property and will be returned to the appropriate first-line supervisor upon separation from DoD IG.

38.12.f. **Equipment Validation.** The UoF PC, in cooperation with DCIS HQ and field personnel, will conduct job task analysis every 3 years to validate required mission requirements dictating the procurement and issuance of uniforms/protective clothing and use of force equipment. Should operational tempo and mission requirements dictate an immediate review of required use of force equipment, the DAIG, INT reserves the right to modify equipment issue to ensure safe and efficient mission execution.

38.12.g. **Procurement of Use of Force Equipment.** When fiscally and operationally appropriate, procurement of Use of Force Equipment will be contracted on a national level. The DCIS Internal Operations Directorate will coordinate with the DoD IG Mission Support Team's Logistics Management Office (MST-LMO) for appropriate contracting support. When operationally dictated to meet mission requirements, the Government Purchase Card may be authorized and/or used in accordance with Inspector General Instruction 4100.33, "Government Purchase Card Program," August 31, 2009, to procure use of force equipment.

38.13. Control Tactics Instructors

38.13.a. **General.** The UoF PM is responsible for managing the DCIS Control Tactics Program and the activities of the agency's coordinators and instructors. Special agents are responsible for maintaining high professional standards in control tactics training.

38.13.b. **Control Tactics Instructor Training.** Only FLETC-certified instructors will conduct control tactics training. Control tactics instructors will complete the Law Enforcement Control Tactics Instructor Training Program (LECTITP). It is recommended, bound by fiduciary control and course availability, that instructors will maintain proficiency and expertise in law enforcement control tactics by completing a FLETC-sanctioned refresher course every 5 years. In the absence of a DCIS instructor, the SAC may authorize a FLETC-certified instructor from another agency to provide refresher training to DCIS special agents. Coordinators will ensure that the instructor follows the approved DCIS protocol for control tactics training. The SAC may also authorize instructors to provide control tactics training to other Federal law enforcement special agents/officers. All control tactics instructors must complete Basic First Aid and cardiopulmonary resuscitation (CPR) training from a sanctioned program, must maintain a current certification, and will be certified via DCIS Form 52, Use of Force Training Data.

38.14. Control Tactics Training

38.14.a. **General.** Special agents must complete initial and refresher training on the DCIS Use of Force Policy and control tactics techniques. Before being issued (b)(7)(E), (b)(7)(F) or restraint devices, special agents must complete authorized training for this equipment. Authorized training includes instruction by DCIS, FLETC, or other law enforcement training programs approved by the DAIG, INT. **NOTE:** Although use of force training also includes firearms, this section does not pertain to firearms training. Firearms policy, equipment, and training are addressed in other sections of this chapter.

38.14.b. **New Special Agents.** Control tactics instructors will provide all newly employed special agents with DCIS Use of Force Policy and control tactics training. Initial Use of Force Policy and control tactics training for new special agent personnel will be documented via DCIS Form 52, "Use of Force Training Data" (Attachment E). In addition, the special agent's SAC will forward a "NEW SPECIAL AGENT USE OF FORCE TRAINING CERTIFICATION FOR SA XXXX" memorandum (Attachment F) to the UoF PM.

38.14.c. **Refresher Training.** Instructors will provide refresher training relative to the DCIS Use of Force Policy on a quarterly basis and control tactics on an annual basis. SACs must ensure that at a minimum all special agents receive scheduled training on an annual basis. In an

effort to reduce expenditures of agency funds, all reasonable efforts should be made to secure no-cost training venues within commuting distance of the local office. Minimum annual training requirements (noted below) that must be met are further delineated in the DCIS Control Tactics Instructor Training Manual (Attachment G).

38.14.d. **Annual Training Requirements.** Minimum required annual Use of Force/Control Tactics Training Requirements:

38.14.d.(1). Use of Force Briefing

38.14.d.(2). (b)(7)(E), (b)(7)(F)

38.14.d.(3). Weapon Retention

38.14.d.(4). Control Tactics

38.14.d.(5). Arrest Techniques

38.14.e. **Remedial Training.** Any special agent who fails to demonstrate a satisfactory execution of any technique will be provided remedial instruction. Control tactics instructors will document the reasons for the remedial training and the date completed. Any failure to achieve a satisfactory execution of any technique after remedial training will be referred to the special agent's supervisor.

(b)(7)(E), (b)(7)(F)

38.14.h. **Restraint Devices.** Special agents are provided agency-issued handcuffs. Special agents are encouraged to carry handcuffs while armed. The use of nonconventional or improvised restraint devices will be used only if it is reasonable and safe to secure a subject in an emergent situation.

38.14.i. **Authorized Absences.** Special agents will complete required refresher training, unless excused by their SAC. The SAC will submit a memorandum granting authorized excused absence from refresher training for:

38.14.i.(1). Significant operational needs,

38.14.i.(2). Medical reasons,

38.14.i.(3). Deployment,

38.14.i.(4). Budgetary constraints, or

38.14.i.(5). Other exigent circumstances.

All memoranda will be electronically forwarded to the UoF PM and the cognizant instructor for file retention. Absences due to medical reasons are addressed in paragraph 38.22.p. The instructor will also document the agent's absence on the current-year DCIS Form 52 (Attachment E). The UoF PM shall maintain copies of all excused absences. Examples of the required format for excused absences can be found in the "Use of Force" folder on the shared drive at S:\DCIS\Use of Force Program.

38.14.j. Training Records. Instructors will maintain all Forms 52 for the personnel under their responsibility. The instructor cadre will certify qualifications, familiarizations, briefings, and additional/remedial training each quarter on Forms 52. Within (10) working days of the close of each quarter, each Field Office Control Tactics Coordinator will ensure pertinent data is transferred to a password-protected spreadsheet for their respective office or HQ on the shared drive at S:\DCIS\Use of Force Program. Within (30) working days of the close of the fiscal year, the SAC will complete the "Annual Special Agent Use of Force Training Certification," (Attachment H). All original DCIS Forms 52 will be maintained permanently during the agent's tenure. An agent's Forms 52 file will follow the agent upon transfer to other DCIS offices. An e-mail may be used as backup documentation should an agent qualify with an instructor who is not the regular instructor in control of the agent's Form 52. Upon departure (e.g., retirement, termination, interagency transfer) from DCIS, all Forms 52 will be packaged, retained, and disposed of in accordance with procedures established in coordination with the National Archives and Records Administration (NARA).

38.15. Firearms Authority

38.15.a. Statutory Authorities. Title 10 U.S.C., section 1585, authorizes the Secretary of Defense to prescribe regulations under which DoD civilian employees may carry firearms while assigned investigative duties or other duties as the Secretary may prescribe. DoD Directive 5106.01 authorizes DoD IG personnel to carry weapons in accordance with DoDD 5210.56.

38.15.b. Approval. Approval to carry firearms is granted by the Inspector General, Department of Defense. Firearms will be issued only to special agents who meet the requirements of this chapter. Continued authorization to carry firearms is contingent on meeting and maintaining the prescribed training requirements of this chapter. Under exigent circumstances, supervisory personnel are authorized to suspend authority to carry firearms and are authorized to recover firearms, as further stated in paragraph 38.18.f.

38.16. Firearms Policy

38.16.a. General. DCIS special agents are designated by law as Federal law enforcement officers. Special agents are required to carry firearms at all times when in a duty status in the United States, its territories, or possessions, except where prohibited or where circumstances make

carrying a firearm inappropriate. (See undercover exception, paragraph 38.16.a.(5).) When off duty, special agents can be recalled to law enforcement duties at any time on short notice. Accordingly, special agents are authorized to carry firearms at all times when off duty and when in a leave status. The decision to carry firearms off duty is at the discretion of the special agent. The rules and regulations of carrying a firearm while in a duty status and off duty status are the same.

38.16.a.(1). Special agents will carry their badge and credentials at all times when in possession of a firearm, in accordance with the provisions of this chapter, except when undercover exception, paragraph 38.16.a.(5)., applies. SACs will establish the policy on the wearing of firearms while in office space for special agents under their supervision. Special agents who do not wear firearms while in office spaces will secure those firearms pursuant to section 38.18.

(b)(7)(E), (b)(7)(F)

(b)(7)(E), (b)(7)(F)

(b)(7)(E), (b)(7)(F)

38.16.a.(2). Exposed weapon carry will be at the discretion of the cognizant SAC. Exposed weapons may be appropriate if customary among non-uniformed law enforcement personnel in the local area or based on weather conditions. It is the special agent's responsibility to use discretion and good judgment to employ the most conservative approach. When weapons are exposed, special agents are required to display a belt badge in plain view. Special agents are authorized to wear tactical raid clothing and/or tactical carriers for body armor and equipment that identifies them as law enforcement officers.

38.16.a.(3). In foreign countries, firearms will be carried in accordance with the laws of that country or, where applicable, Status of Forces Agreements and/or Bilateral Security Agreement(s), provided such arrangements have been coordinated with and approved by local U.S. military and foreign authorities. The UoF PM may provide further guidance, in memorandum format, relative to the possession of firearms in each country of operation. DCIS International Operations Directorate will set policy for specific countries.

38.16.a.(4). Special agents are authorized to draw firearms when the special agent believes that the use of a firearm may be required. Such situations include, but are not limited to, arrests or apprehensions and the execution of court orders. Should it become necessary to draw a firearm for any other reason, notify supervisory personnel. Notification to the DAIG, INT will be reported by the cognizant SAC, FO unless a use of force incident described in section 38.8. occurs in which notification will be made as instructed.

38.16.a.(5). Given the unique and unpredictable nature of undercover operations, exceptions to policy are authorized should the undercover or case agent determine that officer or public safety necessitates the exception.

38.16.b. Prohibited Activities. The following activities are specifically prohibited.

38.16.b.(1). Dry firing, with the exception of authorized firearms maintenance/cleaning and training under the direction of a firearms instructor.

38.16.b.(2). Altering the internal or external mechanical operation of a DCIS-issued or authorized personally owned firearm with manufacturer or aftermarket components that change the performance of the weapon. Mounting laser aiming devices and/or aftermarket grips on DCIS-issued duty-carry pistols. Modifications to DCIS issued magazines, to include grip extensions (magazine grip extensions that are serviceable will be authorized until no longer serviceable). Mounting equipment that is not procured by DCIS on DCIS issued long guns.

38.16.b.(3). Consuming alcohol up to 8 hours prior to or while (b)(7)(E), (b)(7)(F)

38.16.b.(4). Carrying a firearm while consuming alcoholic beverages. Exceptions are limited to operationally necessary undercover situations, in accordance with DCIS SAM Chapter 9 (Undercover Operations). Although drinking while undercover is discouraged, it is recognized that an undercover agent or cover team may need to consume alcoholic beverages to protect the safety of the undercover agent or the public, prevent the special agent's true identity from being exposed, or to further criminal enforcement operations.

38.16.b.(5). Carrying a firearm while taking medications that impair motor skills or judgment. The special agent will notify supervisory personnel that the special agent is taking such medications. The cognizant supervisor shall require the special agent to provide written documentation from the prescribing physician of the medication and impairment. The cognizant supervisor will provide the Health and Wellness (H&W) PM the supporting medical documentation. In turn, the H&W PM will forward the documentation to the Federal Occupational Health (FOH), Medical Review Officer (MRO) for a fit-for-duty opinion. The cognizant supervisor, on receiving the FOH MRO opinion, will determine if the special agent can continue to be authorized to carry a firearm while taking the medication and will document the circumstances/basis of the decision by notifying the UoF PM and the H&W PM via departmental memorandum. The special agent can appeal the supervisor's decision to suspend his or her authorization to carry a firearm by submitting a request to the DoD Office of Inspector General Medical Review Board as detailed in SAM paragraph 58.4.h.

38.16.b.(6). Carrying a firearm in violation of the Domestic Violence Amendment to the Gun Control Act, 18 U.S.C. 922 (G) (8) and (9). This amendment applies to persons convicted of a misdemeanor crime of domestic violence or who are subject to certain court-directed restraining orders. These circumstances make continued retention of any firearm or ammunition unlawful, whether Government issued or privately owned. Special Agents will complete the DD Form 2760, "Qualification to Possess Firearms or Ammunition," (See Attachment I), concurrently with their annual law enforcement availability pay (LEAP) certification at the beginning of each calendar year and provide said documentation to their first line supervisor. The DD Form 2760 will be forwarded to HQ Internal Operations Directorate and HCAS for inclusion in the agent's Official Personnel Folder (OPF). Special agents have an ongoing responsibility to notify supervisors of their involvement in any situation that may violate this Act. On notification of a conviction or issuance of certain court-directed restraining orders, the

cognizant SAC will revoke authorization to possess a firearm pending resolution of the situation. The cognizant SAC will then notify the DAIG, INT. Any special agent affected by this Act must immediately relinquish all agency-issued firearms **and** ammunition to supervisory personnel. The supervisor will take possession of the weapon(s) and ammunition and provide them to the appropriate custodian for safekeeping until resolution. Additionally, any special agent affected by this Act must also dispose of any personally owned weapons and ammunition.

38.16.b.(7). Mishandling a firearm, defined as any incident with a firearm, except an actual discharge, in which a special agent has failed to follow the provisions of this chapter and has used the firearm in an unsafe or reckless manner.

38.16.b.(8). Discharging a firearm not related to a use of force incident or training. Any such incident, whether involving injuries or not, must be reported to the immediate supervisor, the UoF PM, and the DAIG, INT. OQAS, IRD will be notified per DoD IG requirements.

38.16.c. **Reporting Requirements.** Special agents are obligated to notify supervisors of the occurrence of prohibited activities. All prohibited activities involving firearms shall be reported in accordance with section 38.10.

38.17. Firearms Standards

38.17.a. The standard agency-issued handgun is a (b)(7)(E), (b)(7)(F) (b)(7)(E), (b)(7)(F) A special agent may carry a personally owned pistol platform when specifically authorized in writing by the cognizant SAC. Attachment J denotes personally owned pistol platforms authorized for duty carry. Only agency-issued ammunition is authorized while in duty status. Agents opting to carry a personally owned weapon (POW) will provide their own magazines (minimum of three), magazine pouches, and holsters conforming to agency guidelines. Before authorizing a POW, a firearms instructor will coordinate with the DCIS FOFC, FICM, and UoF PM and inspect the handgun to verify, at a minimum, that the handgun functions safely with agency-issued ammunition and conforms to manufacturer specifications. The SAC shall transmit a memorandum, "Authorization to Carry a Personally Owned Handgun," (Attachment K), to the FICM. A copy of the memorandum shall be maintained in the agent's firearms qualification file with all Forms 52. Transfers resulting in a change of a SAC will require updated SAC authorization to carry a personally owned weapon.

38.17.b. The cognizant SAC, with notification to the AIGI-INV through the DAIG, INV, and in coordination with the UoF PM, may authorize a special agent to carry more than one handgun concurrently during exigent circumstances. If authorized a backup weapon, special agents are allowed to carry only one authorized backup weapon except when the undercover exception, paragraph 38.16.a.(5), applies. The make and model of all personally owned backup weapons must be authorized in writing by the UoF PM prior to carry. The cognizant SAC can authorize a special agent to both retain and carry the agency-issued handgun and one authorized personally owned firearm, provided the special agent successfully qualifies quarterly with each handgun. Special agents who fail to qualify with either handgun will have their authorization to carry that firearm revoked immediately. The instructor will notify the special agent, the special agent's supervisor, the cognizant SAC, the FOFC, and the UoF PM that this authorization has been revoked.

38.17.c. The cognizant SAC or his/her designee, in coordination with the UoF PM, will determine which special agent(s) will be authorized to carry agency-issued shotguns. The SAC will determine when and under which circumstances shotguns are operationally required. Only special agents who have completed DCIS qualification training will carry agency-issued shotguns. Authorization to carry a shotgun will be permitted after the SAC receives written justification from the special agent's immediate supervisor requesting authorization. Written justification will include the name of the special agent, the type of firearm, the expected duration of the need to carry the weapon, and notification that qualification on that weapon is current. In exigent circumstances, a verbal request from the immediate supervisor may be warranted, and verbal authorization may be granted by the cognizant SAC. The SAC shall notify the UoF PM as soon as practicable. A written justification and authorization shall be documented when reasonably practicable. Upon conclusion of the assignment, shotguns will be returned to inventory as designated by the SAC or designee, with notification to the UoF PM.

38.17.d. Only the SAC or his/her designee will authorize the use of agency-issued automatic weapons in the field. The SAC will determine which special agent(s), in coordination with the UoF PM, are authorized to carry an automatic weapon. The SAC will also determine when and under which circumstances these weapons are operationally required. DCIS special agents are authorized to carry automatic weapons when requested by partner agencies, or when local conditions exist to make it prudent to have special agents armed with automatic weapons. Authorization to carry an automatic weapon will be permitted only after the cognizant SAC receives written justification from the special agent's immediate supervisor requesting authorization. Written justification will include the name of the special agent, the type of firearm, the expected duration, and notification that qualification on that weapon is current. In exigent circumstances, a verbal request from the immediate supervisor may be warranted, and verbal authorization may be granted by the cognizant SAC. The SAC shall notify the UoF PM as soon as practicable and a written justification and authorization shall be documented when reasonably practical. Upon conclusion of the assignment, automatic weapons will be returned to inventory as designated by the SAC or designee, with notification to the UoF PM.

38.17.e. The cognizant SAC, FO with the concurrence of the DAIG, INV, through coordination with the Program Director, Special Operations; the Undercover PM; and the UoF PM, may approve requests for special agents to carry undercover handguns different from the agency-issued handgun. Formal request procedures can be found in DCIS SAM Chapter 9, "Undercover Operations."

38.18. Firearms Security/Safety

38.18.a. **General.** Special agents are personally responsible for controlling and securing agency-issued firearms and personally authorized handguns.

38.18.b. **Firearms Security/Storage.** During work hours, agency-issued and authorized personally owned handguns may be temporarily stored in the office in locked containers such as special agents' desks or file cabinets, provided non-authorized personnel cannot access the

containers. In offices where access by non-authorized personnel is possible, firearms must be secured in a locked container such as a heavy file cabinet, safe, or “day locker.” To prevent discharges, firearms should remain loaded during temporary storage.

38.18.b.(1). Secure firearms for overnight storage in Class 5 safes. Automatic weapons will be stored only in accordance with DoD Instruction 5100.76. When required, cognizant SACs may request a waiver or exception to DoD Instruction 5100.76 from the DoD OIG Security Manager. On a case-by-case basis, the cognizant SAC may authorize DCIS offices to store firearms that are not agency-issued firearms or **authorized** personally owned handguns in DCIS safes. In these instances, the field office supervisor and/or his/her designee will document the approval and maintain the inventory on file.

38.18.b.(2). Firearms can be secured temporarily in an unattended vehicle by locking them in the trunk of vehicles so equipped. In vehicles without a trunk, firearms can be temporarily stored in a fixed container such as a locking glove compartment, center console, or under-seat compartment; or secured to a permanent vehicle fixture. Shotguns may be secured temporarily in a locked vehicle equipped with weapon mounts (racks) or secured with a case-hardened chain and padlock. All such temporary storage containers or methods must be designed to defeat unauthorized access to firearms. Overnight storage of handguns and shotguns in a vehicle is authorized only when the weapons are secured inside a safe or locking container designed for such purposes, permanently affixed to the vehicle. Overnight storage of automatic weapons in a vehicle is prohibited.

38.18.b.(3). Storage of firearms in foreign countries will be in accordance with the specific country’s laws, or where applicable, the Status of Forces Agreements and/or Bilateral Security Agreement(s), provided such arrangements have been coordinated with and approved by local U.S. military and foreign authorities.

38.18.b.(4). For storage other than described above, all firearms will be secured by one or more of the following recommended methods.

38.18.b.(4).(a). Place the firearm in a security box and lock it. The firearm may be loaded or unloaded. (b)(7)(E), (b)(7)(F)

(b)(7)(E), (b)(7)(F)

38.18.b.(4).(b). Attach a cable lock through the top of the unloaded firearm and through the magazine well to lock it.

38.18.b.(4).(c). Attach a trigger lock to the unloaded firearm.

38.18.b.(4).(d). Disassemble the firearm, secure the frame in one location, and secure the slide and ammunition in another, or otherwise secure the firearm and make it inoperable.

NOTE: To make a firearm safe, remove the source of ammunition, clear the chamber of any live round, and visually and physically inspect the firearm.

38.18.b.(5). In accordance with executive memorandum EM3, “Memorandum on Child Safety Lock Devices,” March 5, 1997, DCIS special agents are provided and are required to use child safety lock devices (as specified in paragraphs 38.18.b.(4).(a). through (c).) for all firearms.

38.18.c. **Loading/Unloading Firearms.** The need to load or unload a firearm in the office should be minimized. All offices must have a prescribed area removed from the presence of non-agent personnel for the safe loading, unloading, cleaning, and examination of firearms. Each prescribed safe area should include a bullet-trap safety device. Special agents will not load or unload firearms in the office other than in this prescribed area.

38.18.d. **Inventory Control**

38.18.d.(1). Overall, the UoF PM is responsible for the inventory of agency firearms. The UoF PM may opt to delegate administration of the firearms inventory to the DCIS FICM. Firearms coordinators and instructors are responsible for ensuring their inventory records are current, complete, and accurate. At each quarterly firearms qualification, instructors will conduct a physical inventory and inspection of all assigned DCIS-issued weapons and authorized personally owned weapons. All instructors who are assigned multiple long guns, FX, and training weapons will conduct a physical inventory and inspection quarterly. Instructors will ensure serial numbers reconcile with what is recorded in the Defense Property Accountability System (DPAS) inventory and on the individual agent’s DCIS Form 52. The FOFCs will be responsible for reporting their inventory findings to the FICM by the end of the first month for each quarter via e-mail. All firearms instructors and coordinators that maintain more than one agency weapon in inventory will complete an annual refresher on accountability and inventory control by reading IGDINST 4140.1, “Property Management Program,” and DoD Instruction 5100.76, which are found on the shared drive at S:\DCIS\Use of Force Program. These instructors will self-certify completion on the Form 52. Not later than March 31 annually, the SACs must reconcile to the UoF PM and the FICM the accuracy of all firearm inventories. The UoF PM and FICM will certify through a memorandum to DAIG, INT, the full accountability of the inventory.

38.18.d.(2). Special agents are issued firearms by serial number. Firearms **WILL NOT** be reissued, lent, or reassigned without prior approval of the FICM and/or the UoF PM. When a DCIS-issued firearm is assigned, reassigned, recovered, or transferred from one office to another, an electronic IG Form 5000.64-1, “Accountable Property Hand Receipt,” will be completed and a copy provided to the FICM and/or UoF PM. The FICM will update changes to the inventory in DPAS and maintain current IG Form 5000.64-1 forms. Access to DPAS is limited to the FICM and UoF PM. If an agent’s authorization to carry a firearm is revoked, the FOFC, FICM, and UoF PM will be notified so that inventory records can be updated.

38.18.d.(3). DCIS offices are authorized to have additional agency-issued firearms in their inventory. DCIS offices will not obtain any weapons through purchase, loan, seizure, or donation for agency use as duty carry or “flash” without first being specifically authorized by the DAIG, INT **and** DAIG, INV. Coordination will be made through the UoF PM, FICM, and in the case of “flash,” the Undercover PM.

38.18.e. Recovery of Firearms. Upon termination of employment, the special agent will relinquish all agency-issued firearms and ammunition to the supervisor. The supervisor will notify the FOFC, FICM, and UoF PM of the recovery within 24 hours. The firearm and ammunition will be secured in accordance with sections 38.18. and 38.19., respectively, pending further guidance from the FICM. Supervisory personnel will recover agency-issued firearms from special agents released from investigative duties for an extended period of time (e.g., military mobilization, leave without pay, temporary medical condition, or deployment) and submit them to the firearms instructor of the respective field element. Notification of such action must be forwarded to the FOFC, FICM, and UoF PM. Additionally, authorization to carry a personally owned firearm in an official capacity will be revoked during this period.

38.18.f. Withdrawn Authorization to Carry Firearms. Authorization to carry an agency-issued firearm or personally owned handgun will be withdrawn if supervisory personnel determine the special agent is deemed unfit for duty. Under these conditions, supervisory personnel will recover agency-issued firearms. The supervisor will notify the FOFC, FICM, and UoF PM within 24 hours. A report describing the circumstances of this action will be made to the DAIG, INT as soon as feasible.

38.18.g. Lost or Stolen Firearms. Lost or stolen agency-issued firearms and authorized personally owned handguns will be reported immediately to the first-line supervisor. The supervisor, through the appropriate chain of command, shall promptly notify the DAIG, INT, the AIGI-INV, and the FOFC. The AIGI-INV shall notify the AIG-QAS or the QAS Director of Investigations. The FOFC will notify the FICM and UoF PM and will immediately report the loss to the National Crime Information Center (NCIC) and initiate a DD Form 200, Financial Liability Investigation of Property Loss. The requirements for reporting the loss or theft of firearms include memorandum from the employee involved and from the first-line supervisor. Each memorandum will be forwarded separately through the cognizant SAC or Office Director to the DAIG, INT, who will coordinate reporting to the AIG-QAS or the QAS Director of Investigations through the AIGI-INV. See QAS Manual, Chapter 2 for specific QAS reporting requirements and information required in the memoranda.

38.18.h. Shipment of Firearms. Shipment of firearms must be initiated by the FOFC, FICM, or UoF PM. All firearms must be shipped by registered U.S. mail (return receipt) or by an approved commercial carrier that provides tracking and accountability capabilities (e.g., FedEx, UPS). All weapon shipments must be sent "Overnight Priority." Firearms will be unloaded when shipped. **Do not ship ammunition with firearms.** When shipping firearms to a foreign country, send the package to the official base or station using the FPO or APO address to ensure the package remains in the U.S. Postal Service system. The outer wrapper of the package will not indicate its contents. At the time of shipment, notify the receiving party by e-mail, indicating the date and mode of shipment, shipment tracking numbers, firearm types, and serial numbers. The receiving office will certify receipt of the shipment contents by e-mail and complete the required IG Form 5000.64-1. On occasion, shipment of weapons to/from overseas may require deviation from these procedures. Said deviation must be approved by the FICM and/or UoF PM before initiating the shipment.

38.19. Ammunition Standards

38.19.a. **General.** DCIS special agents will use only agency-authorized and issued ammunition designated by the FICM for duty carry. Offices will be notified by separate correspondence as to the exact ammunition authorized. The use or carry of any other ammunition, including personally owned ammunition, is prohibited. Ammunition may be secured in locked DCIS vehicles concealed in locked trunks, glove compartments, or other safe, concealable locations.

38.19.b. **Training Ammunition.** During firearms training, some ranges require the use of lead-free ammunition. All training ammunition must have similar ballistic and trajectory characteristics as the duty-carry ammunition. Firearms instructors must ensure that this ammunition is NOT used for duty carry.

38.19.c. **Ammunition Procurement.** Ammunition will be procured by means of a DoD IG contract and will be drop shipped to the respective field elements on a quarterly or semi- annual basis. The FICM will provide guidance on authorized ammunition and purchases. DCIS/DoD IG offices will provide secure storage of ammunition in accordance with DoD Instruction 5100.76.

38.19.c.(1) **Ammunition Inventory Control.** Upon receipt of procured ammunition, the individual field elements (FO, RA, POD) will certify, via email, the quantity and type of ammunition delivered. Copies of all shipping documents will be copied and provided to the FICM. The FICM will reconcile the ammunition that was delivered with the procurement contract.

38.19.c.(2) **Ammunition Inventory Forms.** Any DCIS field element (FO, RA, POD) in possession in excess of (250) rounds of ammunition will maintain Ammunition Inventory Forms via the DCIS Form 53a - .40 caliber (Attachment L), DCIS Form 53b – 12 gauge (Attachment M), DCIS Form 53c – 5.56 millimeter (Attachment N), and/or DCIS Form 53d – 9 millimeter (See Attachment O). During the first and third quarter of the fiscal year, the FOFC will consolidate the ammunition inventory forms and submit them to the FICM for reconciliation and future ammunition procurement projections.

38.19.d. **Ammunition Malfunctions.** Report any significant or recurring ammunition malfunction to the FICM. Malfunctioning ammunition will be pulled from service and secured pending further guidance from the UoF PM.

38.20. Holster Standards. DCIS-authorized holsters must safely retain the firearm and cover the trigger guard, except when undercover exception, paragraph 38.16.a.(5)., applies. Special agents will be provided a holster for their agency-issued handgun. Special agents may purchase other DCIS-authorized holsters at their own expense. Authorized holsters include hip, shoulder, fanny pack, ankle, small of the back, and tactical holsters. The use of level II retention, auto lock-trigger finger release style holsters is prohibited. The carry of handguns in a manner other than in holsters (e.g., loose in purses or briefcases) is prohibited.

(b)(7)(E), (b)(7)(F)

(b)(7)(E), (b)(7)(F)

Special agents will qualify with each authorized handgun using the primary duty holster and will complete annual familiarization training with any alternative holster being used for duty carry.

38.21. Firearms Instructors

38.21.a. **General.** The UoF PM is responsible for oversight of the DCIS Firearms Program and the activities of the agency's firearms coordinators and instructors. Special agents are responsible for maintaining high professional standards in firearms training.

38.21.b. **Firearms Instructors.** FLETC-certified firearms instructors must conduct DCIS firearms training and qualifications. Firearms instructors must complete the FLETC Firearms Instructor Training Program. To maintain proficiency and expertise in firearms instruction, it is recommended, bound by fiduciary control and course availability, that instructors complete a FLETC sanctioned refresher or advanced instructor training course every 5 years. Firearms instructors who have received automatic weapon instructor training at FLETC, or instructors who receive training from another instructor who has completed automatic weapon instructor training at FLETC, are authorized to provide automatic weapon training and qualification to special agents. All firearms instructors must complete Basic First Aid and CPR training from a sanctioned program and must maintain a current certification, which will be certified via the DCIS Form 52, Use of Force Training Data.

38.21.b.(1). When conducting live-fire pistol training, the minimum ratio will be one instructor for every six shooters. When conducting live-fire long gun training, the minimum ratio will be one instructor for every four shooters. Full auto fire and dynamic movement requires a ratio of one instructor per shooter. In the absence of a DCIS firearms instructor, the cognizant SAC may authorize a FLETC-certified firearms instructor from another agency to qualify DCIS special agents. Federal Bureau of Investigation (FBI) and Drug Enforcement Administration (DEA) certified firearms instructors are also permitted to provide refresher firearms training and certification. Other agency instructors may also be used to supplement DCIS firearms instructors to meet the minimum instructor-to-shooter ratio. The SAC may authorize DCIS firearms instructors to provide firearms training to other Federal law enforcement special agents/officers. To reduce expenditures of agency funds, all reasonable efforts should be made to secure no-cost training venues within commuting distance of the local office. If no other firearms instructor is available, qualified firearms instructors are authorized to qualify themselves for all courses of fire; however, it is recommended that another person be present for safety and/or emergency response.

38.21.b.(2). Firearms instructors may have their blood lead levels checked during Federal Occupational Health (FOH) examinations. The test is termed "Blood Lead and ZPP."

38.22. Firearms Training

38.22.a. **General.** The objective of firearms training is to provide special agents with the knowledge, skills, and abilities to effectively employ the use of firearms when objectively reasonable to do so.

38.22.b. **New Special Agents.** Prior to being issued a firearm or authorized to carry a firearm in the performance of their duties, all new special agents must meet the following requirements.

38.22.b.(1). Complete the FLETC Criminal Investigator Training Program or equivalent Federal training program. **NOTE:** The DAIG, INT will approve acceptable training from academies other than FLETC.

38.22.b.(2). Receive instruction in the DCIS Use of Force Policy and all requirements of this chapter.

38.22.b.(3). [REDACTED] (b)(7)(E), (b)(7)(F)
[REDACTED] (b)(7)(E), (b)(7)(F)

38.22.b.(4). Pass the DCIS Pistol Operators Qualification Course (POQC) with an agency-issued weapon or approved personally owned weapon.

38.22.c. **Reporting Requirements.** Initial firearms training for new special agents will be documented on a DCIS Form 52. In addition, the cognizant SAC will forward the required memorandum (Attachment F) to the UoF PM as set forth in paragraph 38.14.b. above.

38.22.d. **Refresher Training.** Special agents must successfully complete quarterly firearms refresher training. Before each training session, special agents will be briefed on safety procedures and the DCIS Use of Force Policy. Firearms instructors will perform a function check of all firearms, examine for defects, ensure the firearms are authorized, and verify all serial numbers. Supervisors will ensure firearms instructors are provided adequate time for training.

38.22.e. **Courses of Fire.** All special agents will successfully complete the following courses of fire.

38.22.e.(1). Pistol Operators Qualification Course (POQC) on a quarterly basis. Agents assigned overseas, will complete the POQC twice annually. Once annually complete the POQC while wearing a ballistic vest or jacket. The special agent should annually complete the POQC with an alternate holster if applicable.

38.22.e.(2). Down and Disabled Officer Course (DDO) once per fiscal year.

38.22.e.(3). Low Light (LL) once per fiscal year.

38.22.e.(4). Shotgun Qualification Course (SQC) every quarter for special agents authorized to carry the agency-issued shotgun.

38.22.e.(5). Rifle Qualification Course (RQC) every quarter for special agents authorized to carry the agency-issued rifle.

38.22.e.(6). Shotgun and rifle familiarization (SFC and RFC) training once per fiscal year for all other agents not authorized to carry the agency-issued shotgun or rifle.

38.22.e.(7). The Tactical Engagement Qualification Course (TEQC) and the Tactical Pistol Course (TPC) were developed by DCIS with guidance from the FLETC Firearms Division as recommended additional (optional) annual training, resources permitting.

38.22.e.(8). All required and optional courses and procedures such as different types of familiarization, judgmental, and simulated firearms training are located on the shared drive at S:\DCIS\Use of Force Program\Current DCIS Qualification Courses.

38.22.f. **Qualification Training.** Special agents must successfully qualify quarterly with each assigned pistol, agency-issued and/or any authorized personally owned handgun. Shooters must achieve a minimum score of 80 percent to pass.

38.22.f.(1). Agents who fire but fail to qualify may NOT be excused from qualifications for the quarter. Remedial training is mandated in this circumstance.

38.22.f.(2). The required quarterly minimum number of rounds to be fired with the handgun is 60. The actual number of rounds fired will be determined by the firearms instructors and based on each special agent's need to qualify and complete necessary familiarization training.

38.22.f.(3). Special agents authorized to carry an agency-issued undercover weapon must achieve a minimum score of 80 percent on the Undercover Agent Course of Fire (UCA-COF) prior to carrying that weapon. While authorized to carry an undercover weapon, the special agent must achieve 80 percent on the UCA-COF each quarter with the holster selected for concealment.

38.22.f.(4). Special agents authorized to carry agency-issued shotguns must qualify quarterly achieving a minimum score of 80 percent on the DCIS SQC. All other special agents are required to complete the shotgun familiarization training course of fire once annually. Special agents authorized to carry agency-issued rifles must fire the RQC course of fire at least quarterly and must achieve a minimum score of 80 percent. All other special agents are required to complete the rifle familiarization training course of fire once annually. Familiarization training will consist of the qualification course of fire without judging accuracy or time.

38.22.f.(5). Special agents will perform a function check at the conclusion of every qualification/familiarization period to ensure weapons are functional for duty carry.

38.22.f.(6). When deemed in the best interest of operations, the DAIG, INT may grant waivers to field supervisors and HQ personnel from agency-required long gun qualifications or familiarization fire. If operationally dictated, personnel assigned in foreign countries may be authorized firearms qualification waivers for handguns and long guns by the cognizant SAC, DAIG, INT, and UoF PM. Waivers will be tracked by the UoF PM.

38.22.g. **Judgmental Training.** It is recommended that firearms instructors coordinate with other law enforcement agencies to identify facilities that may be suitable for judgmental training and training in the use of cover and concealment. If equipment and facilities are available, this training should be provided once a year to supplement the qualification courses of fire.

38.22.h. Simulated Firearms Training. Firearms instructors are encouraged to provide simulated firearms training, using non-lethal training ammunition (NLTA), to special agents on an annual basis. Firearms instructors will coordinate this training with control tactics instructors to ensure the training covers all levels of force. Training will consist of static, interactive, and dynamic drills/scenarios. Firearms coordinators will maintain NLTA equipment, including barrels, ammunition, protective gear, and other training aids. Required equipment can also be obtained via the UoF PM. Annual training will be documented on the DCIS Form 52.

38.22.i. Remedial Training. A special agent who fails to qualify after three attempts will be provided remedial training. The special agent will be allowed three additional attempts to qualify but will not be allowed to fire more than six courses in one day. If the special agent fails to qualify after those six attempts, or if time does not permit additional training on the same day, the special agent will relinquish the firearm to the firearms instructor, and the special agent's supervisor and the UoF PM will be notified. The supervisor will temporarily rescind the special agent's authorization to carry the firearm until the special agent achieves the qualification. The firearms instructor will annotate on the DCIS Form 52 the number of hours and type of remedial training provided.

38.22.j. Additional Training. A special agent who fails to qualify as described above will be provided additional remedial training. After completing this additional training, the special agent will be given the opportunity to qualify. If he or she again fails to qualify, the supervisor will recover the issued firearm and rescind the special agent's authorization to carry both the agency-issued firearm and any personally owned handgun. Supervisory personnel will document the suspension and recovery and notify the appropriate chain of command and FOFC. The supervisor shall seek additional guidance from the UoF PM as to an appropriate course of action. Failure to qualify may be grounds for administrative action, up to and including removal from DCIS.

38.22.k. Unintentional Discharge of Firearm. An unintentional discharge will be reported to the special agent's supervisor and the UoF PM. A special agent who unintentionally discharges a firearm is required to complete remedial training. A firearms instructor will conduct training under the supervision of the firearms coordinator and with guidance from the UoF PM. Training will be provided to address the needs identified by the incident.

38.22.l. Practice Range Facilities. Special agents may conduct individual firearms practice at ranges approved by firearms instructors. With cognizant RAC approval, local firearms instructors will determine issuance of additional agency ammunition to meet training needs. A firearms instructor must monitor this additional training if it is intended to be remedial in nature. Each range must be equipped with a telephone and first-aid equipment.

38.22.m. Authorized Absences. Special agents will complete quarterly required refresher training unless excused by their SAC. The SAC may e-mail a memorandum granting authorized excused absence from refresher training for:

38.22.m.(1). significant operational needs,

38.22.m.(2). medical reasons,

38.22.m.(3). deployment,

38.22.m.(4). budgetary constraints, or

38.22.m.(5). other exigent circumstances (e.g., previously scheduled leave, non-operational temporary duty, other scheduled training).

Generally, the SAC may approve only one absence within any four consecutive quarters, unless the absence is due to a temporary medical condition as defined in paragraph 38.22. p. below. Any exigent circumstance that results in more than one absence will be coordinated with the UoF PM. All memoranda will be electronically forwarded to the UoF PM and the cognizant instructor for file. The instructor will also document the agent's absence on their current year DCIS Form 52 (Attachment E). The UoF PM will maintain all excused absence memorandums. Examples of the required format for excused absences can be found in the "Use of Force" folder on the shared drive at S:\DCIS\Use of Force Program.

38.22.n. Training Records. Instructors will maintain all Forms 52 for the personnel under their responsibility. The instructor cadre will certify qualifications, familiarizations, briefings, additional/remedial training, and pistol(s) serial number verification each quarter. For firearms training, only a PASS (P) or FAIL (F) will be recorded on the Form 52. Within (10) working days of the close of the quarter, each Field Office Firearms Coordinator will ensure pertinent data is transferred to a password-protected spreadsheet for their respective office on the shared drive at S:\DCIS\Use of Force Program. The SACs will verify the data is uploaded by the Field Office Firearms Coordinator. Per the Managers' Internal Control Program (MICP), the SAC will provide a consolidated list (within 15 working days of the close of the quarter) of personnel who were granted a waiver and did not complete the quarterly pistol qualification (QPC), Inventory & Inspection (I&I), and/or Use of Force Briefing (UoFB) via an email to the FICM and UFPM. Within (30) working days of the close of the fiscal year, the SAC will complete the "Annual Special Agent Use of Force Training Certification" (Attachment H). All original DCIS Forms 52 will be maintained during the agent's tenure. An agent's Forms 52 file will follow the agent upon transfer to other DCIS offices. An e-mail may be used as backup documentation should an agent qualify with an instructor who is not the regular instructor in control of the agent's Form 52. Upon departure (e.g., retirement, termination, interagency transfer) from DCIS, all Forms 52 will be packaged, retained, and disposed of in accordance with procedures established in coordination with the National Archives and Records Administration (NARA).

38.22.o. Suspension of Authorization. The cognizant SAC will suspend authorization to carry firearms for any special agent who misses qualification as stated in paragraph 38.22.f., unless the absence is due to a temporary medical condition or other approved absence. The SAC will notify the special agent and the UoF PM in writing that authorization has been suspended. The special agent must immediately relinquish the agency-issued firearm and ammunition to the immediate supervisor and may not carry a personally owned handgun in an official capacity until qualification is accomplished.

38.22.p. Temporary Medical Conditions. A special agent must notify supervisory personnel if/when the special agent has a physical or psychological condition (including use of prescribed medications) that impairs the special agent's ability to carry a firearm and/or engage in

firearms or control tactics training. A special agent with a temporary medical condition (including pregnancy) is permitted to participate in training provided that the special agent's physician furnishes a written statement with concurrence of the agency's MRO that participation would not be harmful to his/her health or dangerous to others. A temporary medical condition includes the following.

38.22.p.(1). Any condition that physically or psychologically impairs the special agent's ability to carry/use a firearm and engage in firearms training. In this instance, the agency-issued firearm will be recovered from the special agent, and the authorization to carry a firearm, including a personally owned handgun, will be suspended during the duration of this condition.

38.22.p.(2). Any condition that does not physically impair a special agent's ability to carry/use a firearm but makes participation in live-fire firearms training and control tactics training inadvisable for medical reasons (including pregnancy). The special agent may be excused from live-fire firearms training and control tactics training at the discretion of the cognizant SAC.

38.22.p.(3). The cognizant SAC may require a special agent to obtain written verification from a licensed medical professional of the existence of the temporary medical condition and its effect on the special agent's ability to perform official duties. Reported changes in a special agent's medical condition will be forwarded to the agency's MRO for review. No special agent with a temporary medical condition that meets the criteria of paragraph 38.22.p. will be required to relinquish his/her firearm, unless the special agent has not qualified for a 12-month period or documented medical circumstances dictate otherwise. If a special agent fails to qualify due to a medical condition that is recurring or exists for a period longer than 12 months, the medical condition may be chronic or permanent in nature. In this circumstance, the cognizant SAC will request the UoF PM and the DAIG, INT to obtain guidance from the agency MRO.

38.22.q. Familiarization Firing for Federal Employees (Other Than DCIS Special Agents) and for State or Local Law Enforcement Personnel

38.22.q.(1). Occasionally, it may be appropriate in the furtherance of the overall DCIS mission to authorize familiarization firing of DCIS weapons by other Federal employees and by state or local law enforcement officers (hereafter referred to as "guests"). The purpose of providing such familiarization firing is to provide these guests an understanding of: (1) the operating characteristics of DCIS weapons; (2) the weapons' actual capabilities and limitations under simulated operational conditions; (3) the type and quality of firearms training received by, and the level of firearms proficiency required of DCIS special agents; and (4) the Use of Force Policy under which a DCIS special agent may employ those weapons. In addition, affording such an opportunity to guests encourages and enhances interagency cooperation and coordination in other joint law enforcement efforts.

38.22.q.(2). The SAC may authorize familiarization firing of DCIS weapons by a guest. Prior to being allowed to fire any DCIS weapon, each guest shall:

38.22.q.(2).(a). execute a General Release Agreement (Attachment P);

38.22.q.(2).(b). receive a safety briefing from an on-site firearms instructor;
and

38.22.q.(2).(c). demonstrate, to the satisfaction of the senior firearms instructor on site, his/her ability to safely handle and operate the weapon(s) to be fired.

38.22.q.(3). A dedicated firearms instructor shall be assigned to each guest, except one who is a law enforcement officer authorized to carry weapons by his/her individual department, during the course of any familiarization firing. This is to both assist the guest in the proper handling and operation of the weapon and to ensure the guest follows all safety procedures. When the guest is a law enforcement officer authorized to carry weapons by his/her department, that guest may be treated as a DCIS special agent at the discretion of the senior firearms instructor on site, for the purpose of determining the maximum permissible “shooter to firearms instructor” ratio on the firing line. For all safety-related purposes (e.g., use of eye and ear protection, application of range safety rules and procedures), guests shall be treated in the same manner as DCIS special agents.

38.22.r. **Retired Agent Qualifications.** DCIS shall not provide firearms or firearms qualifications testing for retiring or retired law enforcement officers or reimburse any costs associated with qualification requirements for retiring or retired law enforcement officers, in accordance with DoD Instruction 5525.12.

38.23. Firearms Maintenance

38.23.a. **General.** The FICM has overall responsibility for the proper functioning of agency-owned firearms. Only the manufacturer or certified armorer will complete repairs and service. Armorer certification will be based on the firearm manufacturer’s recommendations and must be current. All repairs, maintenance, and service procedures will be performed only as specified by the manufacturer of the firearm.

38.23.b. **Maintenance.** The special agent is responsible for routine maintenance (care and cleaning) of agency-issued and authorized personally owned handguns. Armorer inspections of agency and personally owned weapons (b)(7)(E), (b)(7)(F) will be executed every 5 years or 5,000 rounds. All firearms (Government Owned Weapon [GOW] and POW) will undergo a functions test and visual inspection by a firearms instructor *prior* to each qualification. Results of the functions test and visual inspection (Pass or Fail) will be recorded on the DCIS Form 52 in the “(P/F)” column with the action noted as “Weapon Inventory/Inspection.” Weapons failing a functions check and/or visual inspection will be “deadlined” until repaired to meet manufacturer specifications by a DCIS armorer or an authorized manufacturer armorer. DCIS Form 52 will be used to track the armorer inspection dates, and if desired, can be used to track ammunition expenditures for the agent’s assigned weapon.

38.23.c. **Personally Owned Handguns.** The special agent is responsible for repairs and service to authorized personally owned handguns. Required service and armorer inspections will be conducted by a manufacturer certified armorer. All service records will be reviewed by the respective firearms instructor and annotated on the DCIS Form 52.

ATTACHMENTS

- A. Procedure for Obtaining Emergency Legal Representation for DCIS Personnel Involved in “Critical Incidents”
- B. Uniform Categories
- C. DCIS Form 83, DCIS Use of Force and Protective Equipment Hand Receipt
- D. Individual Deployment Kit (IDQ)
- E. DCIS Form 52, Use of Force Training Data
- F. Sample Memorandum for New Special Agent Use of Force Training Certification
- G. DCIS Control Tactics Instructor Training Manual
- H. Sample Memorandum for Annual Special Agent Use of Force Training Certification
- I. DD Form 2760, Qualification to Possess Firearms or Ammunition
- J. Authorized Personally Owned Weapons
- K. Sample Memorandum for Authorization to Carry a Personally Owned Handgun
- L. DCIS Form 53A, DCIS .40 Caliber Ammunition Inventory
- M. DCIS Form 53B, DCIS 12 Gauge Ammunition Inventory
- N. DCIS Form 53C, DCIS 5.56 Rifle Ammunition Inventory
- O. DCIS Form 53D, DCIS 9mm Ammunition Inventory
- P. General Release Agreement

ATTACHMENT A

PROCEDURE FOR OBTAINING EMERGENCY LEGAL REPRESENTATION FOR DCIS PERSONNEL INVOLVED IN “CRITICAL INCIDENTS”



DCIS USE OF FORCE PROGRAM

ATTACHMENT A

PROCEDURE FOR OBTAINING EMERGENCY LEGAL REPRESENTATION FOR DCIS PERSONNEL INVOLVED IN CRITICAL INCIDENTS, WHO ARE THE SUBJECT OF FEDERAL, STATE, COUNTY, OR MUNICIPAL CRIMINAL INVESTIGATIONS

A. Background

The Attorney General recently authorized representation of individual Federal employees by private counsel at Department of Justice (DOJ) expense in the immediate aftermath of line of duty “critical incidents” (*i.e., discharge of a weapon or the use of force resulting in serious bodily injury or death*) when the Federal employee becomes the target/subject of a *Federal, state, county, or municipal criminal investigation* into the critical incident. Generally, this authorization *does not* cover situations involving internal agency investigations against the employee arising from the critical incident. Private counsel retained under this authority provides personal-capacity representation to the employee strictly on a temporary basis (not to exceed 7 calendar days unless specifically authorized by DOJ) while DOJ processes the employee’s written request for representation made pursuant to 28 CFR 50.15. Assuming the employee’s written request for representation is approved, responsibility for representing the employee will be transferred to a litigating component of DOJ, typically the local United States Attorney’s Office.

This procedure provides:

1. An explanation of the process for requesting emergency legal representation, together with an “Information Gathering Checklist” for use at the scene of the critical incident. See Section B and Enclosure 1.
2. Information about private attorneys who have agreed to provide representation to Federal employees on this limited emergency basis. See Section C.
3. An explanation of the process for submitting a written Request for Legal Representation, together with a sample Request Letter. See Section D and Enclosure 2.
4. An explanation of the limitations on “long- term” legal representation as opposed to emergency legal representation at DOJ expense. See Section E.
5. Copies of the applicable Code of Federal Regulation subsections. See Enclosure 3.

6.

(b)(5)

ATTACHMENT A

B. Emergency Request Process

Once a Federal, state, county, or municipal criminal investigation of an incident is commenced, the targeted employee should be advised of his/her right to an attorney to represent him/her in connection with the Federal, state, county, or municipal criminal investigation.¹ Once the employee requests an attorney, the senior DCIS special agent present that was *not* personally involved in the incident (normally the SAC/ASAC/RAC) shall be responsible for initiating the request for emergency legal representation and shall undertake the following steps.

- First, he/she shall obtain all available information concerning the circumstances surrounding the incident, particularly information that indicates whether the incident occurred within the scope of employment. See Enclosure 1 for a description of the type of information desired.
- Second, he/she shall obtain the name(s) of the attorney(s) the employee wishes to have represent him/her.²
- Third, he/she shall contact the DoD OIG Office of General Counsel (DoD OIG OGC) by telephone at 703-604-8350. If the incident occurs after normal duty hours, he/she shall contact the Deputy Assistant Inspector General (DAIG), Investigative Operations, DCIS, who will contact a member of the DoD OIG OGC. During this telephone conversation, he/she will brief the DoD OIG OGC or the DAIG, Investigative Operations concerning the circumstances surrounding the incident including, specifically the information identified in the “Information Checklist” portion of Enclosure 1.

On receiving the information about the circumstances of the incident, DoD OIG OGC will contact DOJ Constitutional Torts Branch, who will make the initial determination of entitlement to emergency legal representation, based on the facts as relayed by the senior DCIS special agent on site through, the DoD OIG OGC. Finally, the DoD OIG OGC will advise the senior DCIS special agent on site of the decision by DOJ.

Since the emergency legal representation will not normally be provided for more than 7 calendar days, as soon as any immediate legal issues have been addressed, the employee should prepare a written “Request for Legal Representation,” pursuant to Section D of this procedure.

¹ A request by Federal, state, county, or municipal authorities to interview a DCIS employee involved in the incident usually satisfies the prerequisite for the existence of a Federal, state, county, or municipal criminal investigation targeting the DCIS employee and therefore trigger the entitlement to emergency legal representation described herein.

² 28 CFR 50.16 requires that DOJ approve the hiring of the specific private counsel in advance. Since the availability of any given private attorney is difficult to project, it is recommended that the employee identify the names of several alternatively acceptable attorneys in order of preference, so that DOJ can approve all of them, subject to availability.

ATTACHMENT A

C. List of Available Private Counsel

The employee will receive, from the U.S. Attorney's Office, a list of private attorneys who have agreed to represent Federal employees on this limited emergency basis at a rate not to exceed the current DOJ reimbursement rate.³

Since the employee requesting emergency legal representation will have to be able to identify by name the private attorney he/she wishes to provide emergency legal representation, it is essential that each employee identify in advance the names of those attorneys he/she will wish to represent him/her if the need arises.

D. Request for Legal Representation

The purpose of emergency representation by private counsel is to protect the legal interests/rights of the DCIS employee while DOJ renders a decision on the employee's formal "Request for Legal Representation." Such emergency representation, therefore, will be provided for no longer than 7 calendar days, unless otherwise authorized by DOJ. A sample "Request for Legal Representation" letter is provided at Enclosure 2. This should be completed and forwarded as soon as possible, via fax with a hard copy via regular mail, to:

General Counsel, Office of the Inspector General, Department of Defense
4800 Mark Center Drive, Room 15K26
Alexandria, VA 22350-1500
Fax: 571-372-7495

Upon receipt, DGC (IG) will review the request, coordinate with DCIS management, advise OGC, prepare a recommendation, and forward it to DOJ for action.

E. Limitations on "Long-Term" Representation, as Opposed to Emergency Legal Representation, at DOJ Expense

Title 28 CFR 50.15 and 50.16 outline the circumstances under which DOJ legal representation may be provided in connection with *civil*, *criminal*, and *congressional proceedings* in which Federal employees are sued, subpoenaed, or charged in their individual capacities (see Enclosure 3). Generally, however, DOJ legal representation is ***not available in Federal criminal proceedings against the employee***. Accordingly, if any type of Federal criminal or administrative investigation of the critical incident is commenced against the employee, representation at Government expense may not be granted. In that event, the employee may, at his/her own expense, continue to be represented by the same private attorney that provided the emergency representation. Thereafter, if the Federal investigation against the employee is concluded without any proceedings against the employee involved in the critical incident, he/she may request reimbursement for the expenses of the private attorney that were incurred in connection with the Federal investigation against the employee.

³ The appearance of an attorney's name on this list does ***not*** constitute any form of endorsement or recommendation of said attorney by the DoD OIG, DCIS, or DOJ.

ATTACHMENT A

F. Enclosures

1. Guidance for Information Gathering Concerning Scope of Employment Following a Critical Incident
2. Sample “Request for Legal Representation” letter
3. 28 CFR 50.15 and 50.16
- 4.

(b)(5)

ATTACHMENT A

Enclosure 1

Guidance for Information Gathering Concerning Scope of Employment Following a Critical Incident

Title 28 CFR 50.15(a) provides that a Federal employee may be provided legal representation in civil, criminal, and congressional investigations and proceedings when his/her involvement is in his/her individual capacity and the actions for which representation is requested (1) reasonably appear to have been performed within the scope of the employee's employment and (2) the Attorney General determines that providing legal representation is in the best interest of the United States.

Conduct will generally be considered to be within the scope of employment when:

- the conduct is of the type the employee was employed to perform;
- the conduct occurs during the authorized work time and within the geographic limits of the work area; and
- the conduct is related, at least in part, to achieving the employer's goals.

Restatement (Second) of Agency.

Information Regarding Emergency, Interim Legal Representation

- Representation is only available if the DCIS agent is the subject of a state or local investigation of the critical incident.
- Representation is good for only 7 calendar days after being granted; therefore, the request should not be submitted until the DCIS agent knows when this first meeting/interview with the state/local investigator will be.
- The master list of pre-approved attorneys willing to provide emergency, interim legal representation at the rates allow to be paid by DOJ is held by the DOJ Torts Branch. To identify any pre-approved attorneys in a specific district, call the Torts Branch at 202-616-4140.
- When a request for emergency, interim legal representation needs to be submitted, proceed as follows:
- Call the Torts Branch at 202-616-4140 to alert them that a request will be forthcoming and to obtain the e-mail address of the individual to whom the request should be sent.
- Requests will be made via e-mail.

ATTACHMENT A

- The request should include as many facts about the critical incident as are known. Information drawn from press reports may be used to supplement local gathered information, however, be certain to clearly identify any information taken from press reports.
- In evaluating these requests, DOJ focuses exclusively on whether the Federal law enforcement officer was acting within the scope of his or her employment, whereas for “regular” representation requests, DOJ focuses on two factors: (a) whether the employee was acting within the scope of his or her employment and (b) whether representation is in the best interest of the Government.
- DOJ averages between one and two emergency interim legal-representation requests per year.
- DOJ has never denied emergency, interim legal representation to a Federal law enforcement officer when the officer's parent agency has concluded that the law enforcement officer was acting within the scope of his employment at the time of the critical incident.

ATTACHMENT A

Enclosure 2

[DATE]

Director
Constitutional Tort Staff
Civil Division
U.S. Department of Justice
P. O. Box 7146
Ben Franklin Station
Washington, DC 20044-7146

**THROUGH: Office of General Counsel, Office of Inspector General, Department of
Defense**

Re: Request for Legal Representation

Dear Director:

Pursuant to 28 CFR 50.15, I request the Attorney General of the United States, or his/her agent, designate counsel to represent me in my official and individual capacities in connection with the state and/or local criminal investigation arising out of the *[identify incident for which representation is being requested; e.g., “physical altercation arising out of arrest of John Doe at his home in Cleveland, Ohio, on the afternoon of January 24, 2014,” or “shooting that occurred in the parking lot of F. W. Woods Hardware store in Denver, Colorado on July 17, 2014”]*. I declare that all my actions were performed in my official capacity, within the scope of my official duties, and in a good faith belief that my actions conformed to the law. I am not aware of any pending related Federal criminal investigation.

I understand that:

I am entitled to retain private counsel at my own expense, and that the Department of Defense expresses no opinion whether I should or should not retain private counsel;

If my request for representation is approved, I will be represented by a U.S. Department of Justice attorney; and that

In actions where the United States, any agency, or any officer thereof in his official capacity is also named as a defendant, the Department of Justice is required by law to represent the United States and/or such agency or officer and will assert all appropriate legal positions and defenses on behalf of such agency, officer, and/or the United States;

ATTACHMENT A

The Department of Justice will not assert any legal position or defense on behalf of any employee sued in his individual capacity that is deemed not to be in the best interest of the United States;

Where appropriate, that neither the Department of Justice nor any agency of the U.S. Government is obligated to pay or to indemnify the defendant employee for any judgment for money damages which may be rendered against such employee; but that, where authorized, the employee may apply for such indemnification from his employing agency upon the entry of an adverse verdict, judgment, or other monetary award;

Any appeal by Department of Justice attorneys from an adverse ruling or judgment against the employee may only be taken upon the discretionary approval of the Solicitor General, but the employee-defendant may pursue an appeal at his own expense whenever the Solicitor General declines to authorize an appeal and private counsel is not provided at Federal expense under 28 CFR 10.16; and,

Although at the time this representation is tendered, no conflict appears to exist that would preclude making all arguments necessary to the adequate defense of the employee, if such conflict should arise in the future, the employee will be promptly advised and steps will be taken to resolve the conflict as indicated in paragraph (a) (6), (9) and (10) of 28 CFR 50.15, and by 28 CFR 50.16.

I declare under penalty of perjury that the foregoing is true and correct. (See 28 U.S.C. 1746).

Executed on: **[DATE]**

[NAME OF REQUESTOR]

ATTACHMENT A

Enclosure 3

[Code of Federal Regulations] [Current as of March 20, 2014]

TITLE 28--JUDICIAL ADMINISTRATION

Sec. 50.15 Representation of Federal officials and employees by Department of Justice attorneys or by private counsel furnished by the Department in civil, criminal, and congressional proceedings in which Federal employees are sued, subpoenaed, or charged in their individual capacities.

(a) Under the procedures set forth below, a Federal employee (hereby defined to include present and former Federal officials and employees) may be provided representation in civil, criminal and Congressional proceedings in which he is sued, subpoenaed, or charged in his individual capacity, not covered by Sec. 15.1 of this chapter, when the actions for which representation is requested reasonably appear to have been performed within the scope of the employee's employment and the Attorney General or his designee determines that providing representation would otherwise be in the interest of the United States. No special form of request for representation is required when it is clear from the proceedings in a case that the employee is being sued solely in his official capacity and only equitable relief is sought. (See USAM 4-13.000)

(1) When an employee believes he or she is entitled to representation by the Department of Justice in a proceeding, the employee must submit forthwith a written request for that representation, together with all process and pleadings served upon him, to his immediate supervisor or whomever is designated by the head of his department or agency. Unless the employee's employing Federal agency concludes that representation is clearly unwarranted, it shall submit, in a timely manner, to the Civil Division or other appropriate litigating division (Antitrust, Civil Rights, Criminal, Land and Natural Resources or the Tax Division), a statement containing its findings as to whether the employee was acting within the scope of his employment and its recommendation for or against providing representation. The statement should be accompanied by all available factual information. In emergency situations the litigating division may initiate conditional representation after a telephone request from the appropriate official of the employing agency. In such cases, the written request and appropriate documentation must be subsequently provided.

(2) Upon receipt of the individual's request for counsel, the litigating division shall determine whether the employee's actions reasonably appear to have been performed within the scope of his employment and whether providing representation would be in the interest of the United States. In circumstances where considerations of professional ethics prohibit direct review of the facts by attorneys of the litigating division (e.g. because of the possible existence of inter-defendant conflicts) the litigating division may delegate the fact-finding aspects of this function to other components of the Department or to a private attorney at Federal expenses.

ATTACHMENT A

(3) Attorneys employed by any component of the Department of Justice who participate in any process used for the purpose of determining whether the Department should provide representation to a Federal employee, undertake a full and traditional attorney-client relationship with the employee with respect to application of the attorney-client privilege. If representation is authorized, Justice Department attorneys who represent an employee under this section also undertake a full and traditional attorney-client relationship with the employee with respect to the attorney-client privilege. Any adverse information communicated by the client-employee to an attorney during the course of such attorney-client relationship shall not be disclosed to anyone, either inside or outside the Department, other than attorneys responsible for representation of the employee, unless such disclosure is authorized by the employee. Such adverse information shall continue to be fully protected whether or not representation is provided, and even though representation may be denied or discontinued. The extent, if any, to which attorneys employed by an agency other than the Department of Justice undertake a full and traditional attorney-client relationship with the employee with respect to the attorney-client privilege, either for purposes of determining whether representation should be provided or to assist Justice Department attorneys in representing the employee, shall be determined by the agency employing the attorneys.

(4) Representation generally is not available in Federal criminal proceedings. Representation may be provided to a Federal employee in connection with a Federal criminal proceeding only where the Attorney General or his designee determines that representation is in the interest of the United States and subject to applicable limitations of Sec. 50.16. In determining whether representation in a Federal criminal proceeding is in the interest of the United States, the Attorney General or his designee shall consider, among other factors, the relevance of any non-prosecutorial interests of the United States, the importance of the interests implicated, the Department's ability to protect those interests through other means, and the likelihood of a conflict of interest between the Department's prosecutorial and representational responsibilities. If representation is authorized, the Attorney General or his designee also may determine whether representation by Department attorneys, retention of private counsel at Federal expense, or reimbursement to the employee of private counsel fees is most appropriate under the circumstances.

(5) Where representation is sought for proceedings other than Federal criminal proceedings, but there appears to exist the possibility of a Federal criminal investigation or indictment relating to the same subject matter, the litigating division shall contact a designated official in the Criminal, Civil Rights or Tax Division or other prosecutorial authority within the Department (hereafter "prosecuting division") to determine whether the employee is either a subject of a criminal Federal investigation or a defendant in a Federal criminal case. An employee is the subject of an investigation if, in addition to being circumstantially implicated by having the appropriate responsibilities at the appropriate time, there is some evidence of his or her specific participation in a crime.

(6) If a prosecuting division of the Department indicates that the employee is not the subject of a criminal investigation concerning the act or acts for which he seeks representation, then representation may be provided if otherwise permissible under the provisions of this section.

ATTACHMENT A

Similarly, if the prosecuting division indicates that there is an ongoing investigation, but into a matter unrelated to that for which representation has been requested, then representation may be provided.

(7) If the prosecuting division indicates that the employee is the subject of a Federal criminal investigation concerning the act or acts for which he seeks representation, the litigating division shall inform the employee that no representation by Justice Department attorneys will be provided in that Federal criminal proceeding or in any related civil, congressional, or state criminal proceeding. In such a case, however, the litigating division, in its discretion, may provide a private attorney to the employee at Federal expense under the procedures of Sec. 50.16, or provide reimbursement to employees for private attorney fees incurred in connection with such related civil, congressional, or state criminal proceeding, provided no decision has been made to seek an indictment or file an information against the employee.

(8) In any case where it is determined that Department of Justice attorneys will represent a Federal employee, the employee must be notified of his right to retain private counsel at his own expense. If he elects representation by Department of Justice attorneys, the employee and his agency shall be promptly informed:

(i) That in actions where the United States, any agency, or any officer thereof in his official capacity is also named as a defendant, the Department of Justice is required by law to represent the United States and/or such agency or officer and will assert all appropriate legal positions and defenses on behalf of such agency, officer and/or the United States;

(ii) That the Department of Justice will not assert any legal position or defense on behalf of any employee sued in his individual capacity which is deemed not to be in the interest of the United States;

(iii) Where appropriate, that neither the Department of Justice nor any agency of the U.S. Government is obligated to pay or to indemnify the defendant employee for any judgment for money damages which may be rendered against such employee; but that, where authorized, the employee may apply for such indemnification from his employing agency upon the entry of an adverse verdict, judgment, or other monetary award;

(iv) That any appeal by Department of Justice attorneys from an adverse ruling or judgment against the employee may only be taken upon the discretionary approval of the Solicitor General, but the employee-defendant may pursue an appeal at his own expense whenever the Solicitor General declines to authorize an appeal and private counsel is not provided at Federal expense under the procedures of Sec. 50.16; and

(v) That while no conflict appears to exist at the time representation is tendered which would preclude making all arguments necessary to the adequate defense of the employee, if such conflict should arise in the future the employee will be promptly advised and steps will be taken to resolve the conflict as indicated by paragraph (a) (6), (9) and (10) of this section, and by Sec. 50.16.

ATTACHMENT A

(9) If a determination not to provide representation is made, the litigating division shall inform the agency and/or the employee of the determination.

(10) If conflicts exist between the legal and factual positions of various employees in the same case which make it inappropriate for a single attorney to represent them all, the employees may be separated into as many compatible groups as is necessary to resolve the conflict problem and each group may be provided with separate representation. Circumstances may make it advisable that private representation be provided to all conflicting groups and that direct Justice Department representation be withheld so as not to prejudice particular defendants. In such situations, the procedures of Sec. 50.16 will apply.

(11) Whenever the Solicitor General declines to authorize further appellate review or the Department attorney assigned to represent an employee becomes aware that the representation of the employee could involve the assertion of a position that conflicts with the interests of the United States, the attorney shall fully advise the employee of the decision not to appeal or the nature, extent, and potential consequences of the conflict. The attorney shall also determine, after consultation with his supervisor (and, if appropriate, with the litigating division) whether the assertion of the position or appellate review is necessary to the adequate representation of the employee and

(i) If it is determined that the assertion of the position or appeal is not necessary to the adequate representation of the employee, and if the employee knowingly agrees to forego appeal or to waive the assertion of that position, governmental representation may be provided or continued; or

(ii) If the employee does not consent to forego appeal or waive the assertion of the position, or if it is determined that an appeal or assertion of the position is necessary to the adequate representation of the employee, a Justice Department lawyer may not provide or continue to provide the representation; and

(iii) In appropriate cases arising under paragraph (a)(10)(ii) of this section, a private attorney may be provided at Federal expense under the procedures of Sec. 50.16.

(12) Once undertaken, representation of a Federal employee under this subsection will continue until either all appropriate proceedings, including applicable appellate procedures approved by the Solicitor General, have ended, or until any of the bases for declining or withdrawing from representation set forth in this section is found to exist, including without limitation the basis that representation is not in the interest of the United States. If representation is discontinued for any reason, the representing Department attorney on the case will seek to withdraw but will take all reasonable steps to avoid prejudice to the employee.

(b) Representation is not available to a Federal employee whenever:

(1) The conduct with regard to which the employee desires representation does not reasonably appear to have been performed within the scope of his employment with the Federal government;

ATTACHMENT A

(2) It is otherwise determined by the Department that it is not in the interest of the United States to provide representation to the employee.

(c)(1) The Department of Justice may indemnify the defendant Department of Justice employee for any verdict, judgment, or other monetary award which is rendered against such employee, provided that the conduct giving rise to the verdict, judgment, or award was taken within the scope of employment and that such indemnification is in the interest of the United States, as determined by the Attorney General or his designee.

(2) The Department of Justice may settle or compromise a personal damages claim against a Department of Justice employee by the payment of available funds, at any time, provided the alleged conduct giving rise to the personal damages claim was taken within the scope of employment and that such settlement or compromise is in the interest of the United States, as determined by the Attorney General or his designee.

(3) Absent exceptional circumstances as determined by the Attorney General or his designee, the Department will not entertain a request either to agree to indemnify or to settle a personal damages claim before entry of an adverse verdict, judgment, or award.

(4) The Department of Justice employee may request indemnification to satisfy a verdict, judgment, or award entered against the employee. The employee shall submit a written request, with appropriate documentation including copies of the verdict, judgment, award, or settlement proposal if on appeal, to the head of his employing component, who shall thereupon submit to the appropriate Assistant Attorney General, in a timely manner, a recommended disposition of the request. Where appropriate, the Assistant Attorney General shall seek the views of the U.S. Attorney; in all such cases the Civil Division shall be consulted. The Assistant Attorney General shall forward the request, the employing component's recommendation, and the Assistant Attorney General's recommendation to the Attorney General for decision.

(5) Any payment under this section either to indemnify a Department of Justice employee or to settle a personal damages claim shall be contingent upon the availability of appropriated funds of the employing component of the Department of Justice.

§50.16. Representation of Federal employees by private counsel at Federal expense.

(a) Representation by private counsel at Federal expense or reimbursement of private counsel fees is subject to the availability of funds and may be provided to a Federal employee only in the instances described in Sec. 50.15(a) (4), (7), (10), and (11), and in appropriate circumstances, for the purposes set forth in Sec. 50.15(a)(2).

(b) To ensure uniformity in retention and reimbursement procedures among the litigating divisions, the Civil Division shall be responsible for establishing procedures for the retention of private counsel and the reimbursement to an employee of private counsel fees, including the setting of fee schedules. In all instances where a litigating division decides to retain private counsel or to provide reimbursement of private counsel fees under this section, the Civil Division shall be consulted before the retention or reimbursement is undertaken.

ATTACHMENT A

(c) Where private counsel is provided, the following procedures shall apply:

(1) While the Department of Justice will generally defer to the employee's choice of counsel, the Department must approve in advance any private counsel to be retained under this section. Where national security interests may be involved, the Department of Justice will consult with the agency employing the Federal defendant seeking representation.

(2) Federal payments to private counsel for an employee will cease if the private counsel violates any of the terms of the retention agreement or the Department of Justice.

(i) Decides to seek an indictment of, or to file an information against, that employee on a Federal criminal charge relating to the conduct concerning which representation was undertaken;

(ii) Determines that the employee's actions do not reasonably appear to have been performed within the scope of his employment;

(iii) Resolves any conflict described herein and tenders representation by Department of Justice attorneys;

(iv) Determines that continued representation is not in the interest of the United States;

(v) Terminates the retainer with the concurrence of the employee-client for any reason.

(d) Where reimbursement is provided for private counsel fees incurred by employees, the following limitations shall apply:

(1) Reimbursement shall be limited to fees incurred for legal work that is determined to be in the interest of the United States. Reimbursement is not available for legal work that advances only the individual interests of the employee.

(2) Reimbursement shall not be provided if at any time the Attorney General or his designee determines that the employee's actions do not reasonably appear to have been performed within the scope of his employment or that representation is no longer in the interest of the United States.

(3) Reimbursement shall not be provided for fees incurred during any period of time for which representation by Department of Justice attorneys was tendered.

(4) Reimbursement shall not be provided if the United States decides to seek an indictment of or to file an information against the employee seeking reimbursement, on a criminal charge relating to the conduct concerning which representation was undertaken.

ATTACHMENT B

UNIFORM CATEGORIES

- CAT I: Special Agents – CONUS/OCONUS (permissive environments)
 - (1) Raid jacket with “DCIS/POLICE” markings
 - (1) Pair of protective pants
 - (1) Short-sleeve tee shirt with “DCIS/POLICE” markings
 - (1) Long-sleeve tee shirt with “DCIS/POLICE” markings
 - (1) Pair of over-the-ankle protective boots with safety toe and bloodborne pathogen-resistant coating
- CAT II: Special Agents - OCONUS (non-permissive environments)
 - (4) Pairs of protective pants
 - (2) Short sleeve shirts
 - (2) Long sleeve shirts
 - (4) Synthetic undershirts
 - (1) Parka or jacket (season dependent)
 - (1) Load bearing trouser belt
 - (1) Boonie hat
 - (1) Pair of over-the-ankle protective boots
 - (1) Pair of protective low-cut protective footwear
 - (1) Pair of waterproof socks (season dependent)
 - (1) Poncho
 - (1) Watch cap (season dependent)
 - (1) Sleeping bag
- CAT III: Field Instructors – (Firearms/Control Tactics/Health&Wellness)
 - (1) Short-sleeve tee shirt with “DCIS Instructor” markings
 - (1) Long-sleeve tee shirt with “DCIS Instructor” markings
- CAT IV: FLETC Instructor Cadre
 - (3) Short sleeve “Polo”-style shirts with “DCIS Instructor” markings
 - (3) Mock turtleneck shirts with “DCIS Instructor” markings
 - (3) Short sleeve tee shirts with “DCIS Instructor” markings
 - (2) Long sleeve tee shirts with “DCIS Instructor” markings
 - (3) Pairs of protective pants
 - (3) Pairs of protective shorts (Use of Force personnel only)
 - (1) Sweatshirt with “DCIS Instructor” markings
 - (1) Raincoat/windbreaker style jacket with “DCIS Instructor” markings
 - (1) Pair of protective footwear for use in Physical Techniques Division mat-rooms (Use of Force personnel only)
 - (1) Pair of protective boots (Use of Force personnel only)
 - (1) Load-bearing trouser belt

ATTACHMENT B

- CAT V: FLETC Adjunct Instructors
 - (1) Short-sleeve “Polo”- style shirts with “DCIS Instructor” markings
 - (3) Short-sleeve “Polo”- style shirts with “DCIS Instructor” markings (Extended TDY only)
- CAT VI: Special agents participating in DCIS specific training aboard FLETC
 - (5) “Polo”- style shirts with “DCIS” markings
 - (1) Sweatshirt with “DCIS” markings
 - (1) Windbreaker jacket with “DCIS” markings
 - (3) Pairs of standard FLETC issue BDU pants
 - (1) Web belt
 - (3) Pairs of standard FLETC issue BDU shorts (Use of Force training only)

ACCOUNTABILITY

- Issuance of items in Category (CAT) I, III, IV, V must be annotated in the individual agent’s DCIS Use of Force and Protective Equipment Hand Receipt, Form 83.
- Issuance of items in Category (CAT) II will be accounted for via the Individual Deployment Equipment (IDQ) checklist.
- Issuance of items in Category (CAT) VI will be accounted for via the FLETC Uniform Service Division.

ATTACHMENT E

[illegible]

ATTACHMENT E

SECTION III - INSTRUCTIONS FOR COMPLETING FORM

Instructors will maintain all DCIS Forms 52 for the personnel under their responsibility. The instructor cadre will certify qualifications, familiarizations, briefings, additional/remedial training and pistol(s) serial number verification each quarter. For firearms training, only a PASS (P) or FAIL (F) will be recorded on the DCIS Form 52. Within ninety (90) working days of the close of the fiscal year, each Firearms Coordinator will ensure pertinent data is transferred to a password-protected spreadsheet for their respective office or HQ on the shared drive at S:\DCIS\Use of Force Program. The Coordinator may input data at anytime, but will have final oversight and responsibility for ensuring all annual training requirements have been met by personnel under their responsibility. The Coordinator will then forward results to the cognizant SAC, or component executives, if applicable, who will utilize this data to complete the "Annual Special Agent Firearms Training Certification."

Agents are responsible for initiating a new DCIS Form 52 within (15) days of the start of a fiscal year.

1-11. Fill out the information at the top of the form in its entirety for **each** DCIS Form 52 used; First Name, Last Name, Middle Initial, Office Code, Fiscal Year, Make, Model, and Serial Number of Government-Issued Pistol, Make, Model, and Serial Number of Personally-Owned Weapon (if applicable).

12. Date: The date actual training/briefing/qualification/familiarization takes place.

13. Weapon: GOW or POW (for pistol), shotgun, or rifle.

14. Action: Choose from among the abbreviations in the above listed requirements columns to describe the training completed. In some cases, more than one abbreviation will be used in the "Action" category. If all lines are filled on the Form 52, continue to document training on another Form 52 and keep the forms together, grouped by fiscal year.

15. P/F: Pass/Fail

16. Agent Signature: Signature of the agent completing the training.

17. Instructor Signature: Signature of the instructor certifying the training.

ATTACHMENT F

SAMPLE MEMORANDUM FOR NEW SPECIAL AGENT
USE OF FORCE TRAINING CERTIFICATION



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
DEFENSE CRIMINAL INVESTIGATIVE SERVICE
FIELD OFFICE ADDRESS
CITY, STATE ZIP

April 30, 2010

MEMORANDUM FOR USE OF FORCE PROGRAM MANAGER

FROM: SAC XXXX

SUBJECT: NEW SPECIAL AGENT USE OF FORCE TRAINING CERTIFICATION FOR
SA XXXX

This memorandum certifies that SA XXXX, DCIS XXXX, has successfully completed the new hire Use of Force training protocol delineated in Special Agents Manual, Chapter 38, Use of Force. Specifically, SA XXXX has successfully completed required courses of fire, (b)(7)(E), (b)(7)(F) training, control tactics training, and arrest techniques training. SA XXXX has been provided with the DCIS Use of Force and (b)(7)(E), (b)(7)(F) briefings.

Special Agent XXXX is not affected by the Domestic Violence Amendment to the Gun Control Act/Lautenberg Amendment. Special Agent XXXX further understands that he/she has an affirmative duty to notify supervisory personnel if he/she receives a qualifying conviction in the future.

Special Agent XXXX has been issued a Government-owned XXXX pistol, serial number XXXX. Special Agent XXXX has completed the required protocol to carry a personally owned weapon and is authorized to carry his/her personally owned (b)(7)(E), (b)(7)(F) serial number XXXX.

John/Jane Doe
SAC XXXX Field Office

ATTACHMENT G

DCIS CONTROL TACTICS
INSTRUCTOR TRAINING MANUAL



DCIS USE OF FORCE PROGRAM

ATTACHMENT G

The Training Manual for Control Tactics will consist of the following manuals and documents:

- ❖ FLETC Law Enforcement Control Tactics Instructor Training Program (LECTITP) Training Manual (**required**)

(NOTE: This manual is furnished by FLETC upon completion of the LECTITP.)

- ❖ FLETC Law Enforcement Control Tactics Refresher Instructor Training Program (LECTIRTP) Training Manual (**optional**)

(NOTE: This manual is furnished by FLETC upon completion of the LECTIRTP)

- ❖ Any other training guides or procedures approved by the Deputy Assistant Inspector General (DAIG), Internal Operations in concert with the Use of Force Program Manager (UoF PM).

ATTACHMENT G

CONTROL TACTICS TRAINING

MANDATORY TRAINING METHODS/TECHNIQUES

I. USE OF FORCE BRIEFING*

II. ARREST TECHNIQUES

- A. Threat Assessment
- B. Weapon Recovery
- C. Handcuffing Suspects
- D. Searching Suspects
- E. Escorting Suspects

III. CONTROL TACTICS

- A. Weapon Retention
- B. Strike and Vulnerable Target Areas
- C. Takedowns
- D. Ground Defense

IV. (b)(7)(E), (b)(7)(F) TECHNIQUES V. INJURY MANAGEMENT

VI. EDGED WEAPON DEFENSE

*Firearms Primary Coordination

OPTIONAL CONTROL TACTICS TRAINING METHODS/TECHNIQUES

I. VEHICLE AND ROOM SEARCHES

II. WITNESS/PRISONER TRANSPORTATION

III. TACTICAL SIMULATION TRAINING

ATTACHMENT H

**SAMPLE MEMORANDUM FOR ANNUAL SPECIAL AGENT
USE OF FORCE TRAINING CERTIFICATION**



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
DEFENSE CRIMINAL INVESTIGATIVE SERVICE
FIELD OFFICE ADDRESS
CITY, STATE ZIP

April 30, 2010

MEMORANDUM FOR USE OF FORCE PROGRAM MANAGER

FROM: SAC XXXX

SUBJECT: USE OF FORCE TRAINING, FISCAL YEAR 20XX, XXXX FIELD OFFICE

Unless otherwise noted, all XXXX Field Office personnel have completed the required annual Use of Force training protocol in accordance with Special Agents Manual, Chapter 38, Use of Force.

The following special agents were provided authorized waivers for completion of training.

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

Amplifying information relative to the justification for the waivers is maintained by the DCIS UoF PM.

John/Jane Doe
SAC XXXX Field Office

ATTACHMENT I

QUALIFICATION TO POSSESS FIREARMS OR AMMUNITION

PRIVACY ACT STATEMENT

AUTHORITY: 18 U.S.C. 922(g)(9); E.O. 9397.

PRINCIPAL PURPOSE(S): To obtain information to determine if you have been convicted of a crime of domestic violence which would disqualify you from shipping, transporting, possessing or receiving either Government-issued or private firearms or ammunition and to determine if reassignment, reclassification, detail or other administrative action is warranted. Your Social Security Number is solicited solely for purposes of verifying your identity.

ROUTINE USE(S): To the Department of Justice so that such information can be included in the National Instant Criminal Background Check System which may be used by firearm licensees (importers, manufacturers or dealers) to determine whether individuals are qualified to receive or possess firearms and ammunition.

DISCLOSURE: Mandatory for all personnel who are required to certify. Failure to provide the information may result in (1) (military only) the imposition of criminal or administrative penalties for failing to obey a lawful order, and (2) (civilian only) the imposition of administrative penalties, to include removal from Federal service. However, neither your answers nor information or evidence gained by reason of your answers can be used against you in any criminal prosecution for a violation of Title 18, United States Code, Section 922(g)(9), including (military only) prosecutions under the Uniform Code of Military Justice, based on a violation of Section 922(g)(9), for conduct which occurred prior to the completion of this form. The answers you furnish and any information resulting therefrom, however, may be used against you in a criminal or administrative proceedings if you knowingly and willfully provide false statements or information.

SECTION I - INSTRUCTIONS

An amendment to the Gun Control Act of 1968 (18 U.S.C. 922) makes it a felony for anyone who has been convicted of a misdemeanor crime of domestic violence to ship, transport, possess, or receive firearms or ammunition. It is also a felony for any person to sell or otherwise dispose of a firearm to any person so convicted.

The Department of Defense has, by policy, expanded the prohibitions contained in Title 18 Section 922(g)(9) to those military or civilian personnel who have felony convictions for crimes of domestic violence. Convictions of crimes of domestic violence do not include summary court-martial convictions, the imposition of nonjudicial punishment (Article 15, UCMJ), or deferred prosecutions (or similar alternative dispositions) in civilian courts. Furthermore, a person shall not be considered as having committed a "crime of domestic violence" for purposes of the firearms restriction of the Gun Control Act unless all of the following elements are present:

- (1) the person was convicted of a crime;
- (2) the offense has as its factual basis the use or attempted use of physical force, or threatened use of a deadly weapon;
- (3) the convicted offender was at the time of the offense:
 - (a) a current or former spouse, parent or guardian of the victim,
 - (b) a person with whom the victim shared a child in common,

- (c) a person who was cohabiting with or has cohabited with the victim as a spouse, parent, or guardian, or
- (d) a person who was similarly situated to a spouse, parent, or guardian of the victim;

- (4) the convicted offender was represented by counsel, or knowingly and intelligently waived the right to counsel;
- (5) if entitled to have the case tried by jury, the case was actually tried by jury or the person knowingly and intelligently waived the right to have the case tried by jury;
- (6) the conviction has not been expunged or set aside, or the convicted offender has not been pardoned for the offense or had civil rights restored, unless the pardon, expungement, or restoration of civil rights provides that the person may not ship, transport, possess or receive firearms.

If you have ever received a domestic violence conviction: (1) you may not possess any firearm or ammunition; and (2) you must return any Government-issued firearm or ammunition to your commander or immediate supervisor; and (3) you must take steps to relinquish possession of any privately owned firearms or ammunition. Furthermore, any previously issued authorization to possess a firearm or ammunition is revoked.

If you have any questions, or you are uncertain if you have such a conviction, you may wish to contact a legal assistance attorney, if eligible, or a private attorney, at your own expense.

SECTION II - QUALIFICATION INQUIRY *(Complete and return to your commander or immediate supervisor within 10 days of receipt)*

1. HAVE YOU EVER BEEN CONVICTED OF A CRIME OF DOMESTIC VIOLENCE AS DESCRIBED ABOVE: *(Initial and date)*

YES	NO	I DON'T KNOW <i>(Provide explanation on reverse)</i>
-----	----	--

2. IF YOU ANSWERED "YES" TO THE FIRST QUESTION, PROVIDE THE FOLLOWING INFORMATION WITH RESPECT TO THE CONVICTION:

a. COURT/JURISDICTION	b. DOCKET/CASE NUMBER
c. STATUTE/CHARGE	d. DATE SENTENCED (YYYYMMDD)

3. **CERTIFICATION.** I hereby certify that, to the best of my information and belief, all of the information provided by me is true, correct, complete, and made in good faith. I understand that false or fraudulent information provided herein may be grounds for criminal and/or administrative proceedings, to include (if civilian) adverse action, up to and including removal, and (if military) disciplinary action under the Uniform Code of Military Justice. I further understand that I have a continuing obligation to inform my Commander or Supervisor should I be convicted of a crime of domestic violence in the future.

a. NAME <i>(Last, First, Middle Initial)</i>	b. RANK/GRADE	c. SOCIAL SECURITY NUMBER
d. ORGANIZATION	e. SIGNATURE	f. DATE SIGNED (YYYYMMDD)

ATTACHMENT J

AUTHORIZED PERSONALLY OWNED WEAPONS

Agents authorized to carry Government-owned weapons are authorized to carry personally owned weapons (POW) while in duty status. Authorized weapons must be (b)(7)(E), (b)(7)(F) and limited to manufacturers noted below.

- (b)(7)(E), (b)(7)(F)

ATTACHMENT K

**SAMPLE MEMORANDUM FOR AUTHORIZATION TO
CARRY A PERSONALLY OWNED HANDGUN**



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
DEFENSE CRIMINAL INVESTIGATIVE SERVICE
FIELD OFFICE ADDRESS
CITY, STATE ZIP

April 30, 2010

MEMORANDUM FOR SPECIAL AGENT IN CHARGE, XXXX FIELD OFFICE

SUBJECT: Authorization to Carry a Personally Owned Handgun

In accordance with Chapter 38 of the Defense Criminal Investigative Service (DCIS) Special Agents Manual, I request authorization to carry the below described handgun:

Manufacturer: _____ Model Number: _____
Serial Number: _____ Barrel Length: _____
Caliber: _____

I certify that I am not affected by the Domestic Violence Amendment to the Gun Control Act. I further understand that I have an affirmative duty on an ongoing basis to notify my supervisor if I receive a qualifying conviction in the future. I also understand that at the discretion of the SAC, the authorization to carry a personally owned handgun may be revoked.

Signature: _____ Date: _____
Special Agent, DCIS

=====

CERTIFICATION: SA XXX has met all training requirements of Chapter 38 as pertains to the carry of a personally owned handgun as specified above. The handgun has been inspected and meets all requirements.

Firearms Instructor: _____ Date: _____

Approved: _____ Disapproved: _____ Date: _____

Special Agent in Charge

ATTACHMENT L

DEFENSE CRIMINAL INVESTIGATIVE SERVICE
(b)(7)(E), (b)(7)(F) AMMUNITION INVENTORY

[illegible]

(b)(7)(E), (b)(7)(F)

ITION INVE

(b)(7)(E), (b)(7)(F)

DEFINITION INVE

ADOBE LIVECYCLE DESIGNER ES

February 2016

ATTACHMENT O

DEFENSE CRIMINAL INVESTIGATIVE SERVICE
(7)(E), (b)(7) AMMUNITION INVENTORY

[illegible]

ATTACHMENT P

GENERAL RELEASE AGREEMENT

This GENERAL RELEASE AGREEMENT (hereinafter referred to as the "Agreement"), made this day ____ day of _____, 20XX, by and between the DEFENSE CRIMINAL INVESTIGATIVE SERVICE, OFFICE OF THE INSPECTOR GENERAL OF THE DEPARTMENT OF THE DEFENSE (hereinafter referred to as "DCIS") and _____ hereinafter referred to as the "Guest,"
(Insert full name of individual participating in familiarization firing)
provides that:

WHEREAS, the Guest desires to participate in familiarization firing of one or more DCIS owned weapons during a regularly scheduled quarterly firearms training session; and,

WHEREAS, DCIS desires to have the Guest participate in familiarization firing of one or more DCIS owned weapons in order to provide the Guest with (1) an understanding of the operating characteristics of DCIS weapons; (2) an understanding of the weapons' actual capabilities and limitations under simulated operational conditions; (3) an understanding of the type and quality of firearms training received by, and the level of firearms proficiency required of, DCIS special agents; and (4) an understanding of the "Use of Force" policy under which a DCIS special agent may employ those weapons;

NOW THEREFORE, WITNESSETH that in consideration of the mutual promises, covenants, and agreements contained herein and other good and valuable consideration, it is hereby agreed by and between the parties as follows:

1. DCIS shall provide the weapon(s), ammunition, safety equipment, safety briefing, and firing range supervision to allow the Guest to participate in familiarization firing of one or more DCIS owned weapons.
2. The Guest, on behalf of himself/herself and his/her heirs and assigns, hereby knowingly and voluntarily assumes all risk of any injury, loss, or damage to persons or property as a result of his/her participation in this familiarization firing, and furthermore agrees to indemnify and hold DCIS, its agents, and/or employees harmless from and against all actions, liability, claims, suits, damages, cost, and expenses of any kind which may be brought against DCIS, its agents, and/or employees as a result of any injury, loss, or damage to persons or property resulting from the negligent actions of DCIS, its agents, and/or employees in connection with this familiarization firing.

DCIS Instructor signature (date)

Guest signature (date)



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

December 14, 2016

MEMORANDUM FOR ALL DCIS SPECIAL AGENTS

SUBJECT: Interim Policy for Special Agents Manual (SAM) Chapter 38, "Use of Force,"
regarding Revised Selection of Personally Owned Weapons Authorized While in
Duty Status

Effective immediately, this interim policy modifies SAM Chapter 38 to expand the selection of personally owned weapons (POW) authorized for use by special agents while in a duty status. Authorized weapons must be (b)(7)(E), (b)(7)(F) and are limited to the manufacturers noted in Attachment A.

Special agents opting to carry a POW will adhere to the guidance delineated in SAM Chapter 38 relative to approval procedures, safety inspections, qualifications, and weapons maintenance. Before the special agent can carry a POW in a duty status, the special agent must qualify with that POW in accordance with SAM Chapter 38. SAM Chapter 38 is hereby amended to include the following.

Special agents authorized to carry a POW will provide their own magazines (minimum of three), magazine pouches, and holsters conforming to agency guidelines. Special Agents in Charge will limit the number of POWs per agent to two (2).

Special agents authorized to carry a POW shall have a manufacturer certified armorer conduct an inspection of the weapon every 5 years or 5000 rounds, whichever occurs first. The special agent is responsible for repairs and service to authorized personally owned handguns. Alterations to the internal or external operating mechanics of handguns from original manufacturer specifications are prohibited. The armorer will provide the special agent with written documentation of the inspection and any repairs completed. The special agent will furnish a copy of that document to the Firearms Inventory Control Manager (FICM).

Specifically, SAM Chapter 38 is amended as follows.

38.17.a. The standard agency-issued handgun is a (b)(7)(E), (b)(7)(F) semiautomatic pistol. Special agents assigned within the 50 United States, its territories, or possessions may arm with two DCIS-approved POWs regardless of duty status. All DoD arming and use of force rules remain in effect for POWs. The POW may be carried during any investigative or operational activity. Prior to requesting authorization to carry a POW, the individual must be qualified with their current duty weapon and current with all arming related training. Attachment A denotes personally owned pistol platforms authorized for duty carry. Only agency-issued ammunition is authorized regardless of duty status. Agents opting to carry a POW must actually own the weapon, and will provide their own magazines (minimum of three), magazine pouches, and holsters conforming to agency guidelines. Before authorizing a POW, a firearms instructor will coordinate with the DCIS Field Office Firearms Coordinator

(FOFC), FICM, and Use of Force (UoF) PM and inspect the handgun to verify, at a minimum, that the handgun functions safely with agency-issued ammunition and conforms to manufacturer specifications. Before the special agent can carry a POW in a duty status, the special agent must qualify with that POW IAW this Chapter. Final approval to carry a POW is granted when the SAC transmits a memorandum, "Authorization to Carry a Personally Owned Handgun," (Attachment K), to the FICM. A copy of the memorandum shall be maintained in the agent's firearms qualification file with all Forms 52. A new approval request will be completed upon change of SAC, permanent change of station (PCS) of an agent (at the gaining office), or when replacing a POW. All DCIS firearms instructors approved to carry a POW are also required to complete quarterly POQC with the Government issued platform.

38.18.d.(1). Overall, the UoF PM is responsible for the inventory of agency firearms. The UoF PM may opt to delegate administration of the firearms inventory to the DCIS FICM. Firearms coordinators and instructors are responsible for ensuring their inventory records are current, complete, and accurate. DCIS-approved POW will not be inventoried as part of the agencies' USG-owned weapons. At each quarterly firearms qualification, instructors will conduct a physical inventory and inspection of all assigned DCIS-issued weapons and authorized personally owned weapons. All instructors who are assigned multiple long guns, FX, and training weapons will conduct a physical inventory and inspection quarterly. Instructors will ensure serial numbers reconcile with what is recorded in the Defense Property Accountability System (DPAS) inventory and on the individual agent's DCIS Form 52. The FOFCs will be responsible for reporting their inventory findings to the FICM by the end of the first month for each quarter via email. All firearms instructors and coordinators that maintain more than one agency weapon in inventory will complete an annual refresher on accountability and inventory control by reading IGDINST 4140.1, "Property Management Program," and DoD Instruction 5100.76, which are found on the shared drive at S:\DCIS\Use of Force Program. These instructors will self-certify completion on the Form 52. Not later than March 31 annually, the SACs must reconcile to the UoF PM and the FICM the accuracy of all firearm inventories. The UoF PM and FICM will certify through a memorandum to DAIG, INT, the full accountability of the inventory.

38.18.d.(2). Special agents are issued firearms by serial number. In the case where a POW is authorized, issuance of, and qualification with, a Government Owned Weapon (GOW) is not required, except in the case of current firearms instructors (see 38.17.a.). Firearms WILL NOT be reissued, lent, or reassigned without prior approval of the FICM or the UoF PM. When a DCIS-issued firearm is assigned, reassigned, recovered, or transferred from one office to another, an electronic IG Form 5000.64-1, "Accountable Property Hand Receipt,"...

Deviations from this policy will be at the discretion of the Deputy Inspector General for Investigations (DIG-INV).

This policy is in effect until it is rescinded or incorporated into the next revision of SAM Chapter 38. Any questions related to this policy should be directed to me at (703) 604-(b)(6), (b)(7)(C)

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

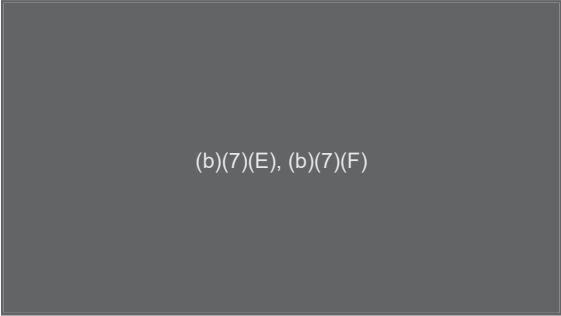
Assistant Director
Defense Criminal Investigative Service

Attachments:
As stated.

ATTACHMENT A

AUTHORIZED PERSONALLY OWNED WEAPONS

Special agents authorized to carry a personally owned weapons (POW) while in a duty status are limited to (b)(7)(E), (b)(7)(F) weapons manufactured by the following.



(b)(7)(E), (b)(7)(F)

CHAPTER 39

BADGES AND CREDENTIALS

<u>Contents</u>	<u>Section</u>
Purpose	39.1.
Types and Description of Credentials	39.2.
Requests for and Issuance of Credentials	39.3.
Reissuance of Credentials	39.4.
Badges	39.5.
Use and Protection of Badges and Credentials	39.6.
Accountability	39.7.
Loss of Badges and Credentials	39.8.
Recovery and Disposition	39.9.
Retired Special Agent Identification Card	39.10.

39.1. Purpose. Defense Criminal Investigative Service (DCIS) credentials are authorized by the Office of the Inspector General of the Department of Defense (OIG DoD) to provide identification for personnel authorized to represent DCIS in conducting investigations of criminal violations and collecting evidence. DCIS credentials appoint and authorize special agents to carry concealed firearms, conduct criminal investigations, make arrests and execute search warrants, gain access to all DoD facilities consistent with the level of security clearance and special accesses of the individual, obtain access to specific records and information, and perform certain functions consistent with conducting official Government business. Inspector General Instruction (IGDINST) 5200.3, “Credential Program,” October 7, 2011, establishes policies, responsibilities, and procedures for the issuance, maintenance, and control of OIG DoD credentials, along with Department of Defense Instruction (DODI) 5525.12, “Implementation of the Amended Law Enforcement Officers Safety Act of 2004 (LEOSA), February 13, 2014. This chapter promulgates policy and procedures regarding issuance and control of DCIS badges and credentials.

39.2. Types and Description of Credentials

39.2.a. Special Agent Credentials. Issued to civilian 1811 series DCIS personnel. Special agent credentials consist of two laminated cards. (b)(7)(E)

(b)(7)(E)

39.2.b. Interim Special Agent Credentials. Issued to new DCIS special agents that have not completed the Criminal Investigator Training Program (CITP) at the Federal Law Enforcement Training Center (FLETC) or a similar course. Interim credentials permit new special agents access to information required to do the work of an 1811; however, they do not include concealed weapon or arrest/search warrant language. Upon graduation from the CITP, new special agents will be presented their permanent DCIS badge and credentials.

39.2.c. **Investigator Credentials.** Issued to certain non-1811 individuals who conduct investigative duties on behalf of DCIS.

39.3. Requests for and Issuance of Credentials. Headquarters (HQ) DCIS/Internal Operations (04) and the OIG DoD Office of Security are responsible for issuance of credentials. In order to facilitate the issuing of credentials to newly hired special agents, the following procedures will be used during the selection process.

39.3.a. Once the applicant has been given an entrance on duty date, return the signed credential sheet and a digital photograph and send them to HQ DCIS/04, which will process the credentials through the Office of Security. The credential sheet is located on the DCIS Admin Toolbox intranet Web page. Field locations should send the photograph and signature sheet via e-mail. (Note: Credential sheets with illegible signatures will be returned to the applicant.) Credentials will be sent by overnight delivery to FLETC for presentation at graduation from CITP or, in the case of a special agent not required to attend CITP, to the office where the applicant will be assigned. Use FedEx, UPS, U.S. Postal Service, or other companies with similar mail-tracking capability to send credentials.

39.3.b. The photographic image of the applicant must be full-face, head and shoulders. A plain white or light blue background will serve as a backdrop. The applicant must be dressed in business attire, and eyeglasses must be worn if the applicant wears them routinely. See IGDINST 5200.3, Chapter 2, Paragraph C. for more specific guidelines.

39.3.c. When requesting Investigator credentials or IG Representative credentials for paid or unpaid interns, the Special Agent in Charge (SAC) or Headquarters Director must also provide HQ DCIS/04 with justification for the credentials.

39.4. Reissuance of Credentials

39.4.a. Credentials bear no expiration date. Credentials will be reissued when their condition is not acceptable or if the photograph no longer portrays a reasonable likeness of the bearer. The growth of a mustache or other substantive change in physical appearance is considered sufficient reason for requesting new credentials, provided such changes are not temporary. Other reasons include a name change and loss or theft.

39.4.b. It is the responsibility of the first-line supervisor to ensure that credential photographs portray a reasonable likeness of the bearer.

39.5. Badges

39.5.a. Badges are issued to special agents along with their DCIS credentials and are issued for the duration of the employee's DCIS career. Special agents shall carry the badge during all periods of duty, unless operational circumstances dictate otherwise.

39.5.b. Each special agent will be issued two badges. (b)(7)(E)

(b)(7)(E)

39.5.c. Surrender all badges and credentials to HQ DCIS/04 upon reassignment to another agency, resignation, or termination from DCIS.

39.6. Use and Protection of Badges and Credentials

39.6.a. Badges and credentials are issued to special agents as a means of identification in the conduct of official Government business, or in the event it is necessary to identify the special agent as a law enforcement officer.

39.6.b. Special agents authorized to carry badges and credentials should not allow them to be removed from their control. Anyone to whom they are displayed for official business is entitled to examine them as closely as is necessary to verify the identification of the special agent, the organization, and/or the scope of authority; however, examination must take place in the special agent's presence.

39.6.c. The special agent is solely responsible for protecting his/her badge and credentials. Safeguarding these items is vital, and each holder must be aware of the serious repercussions that may result from their loss or compromise.

39.6.d. Special agents are on call 24 hours a day, and must have ready access to their badge and credentials after normal working hours. When the badge and credentials are carried, the special agent's conduct must always be reasonable and prudent, so that the integrity and purpose of the badge and credentials are not compromised.

39.6.e. At all times when the special agent deems it appropriate to wear the badge, he or she is acting in an official capacity and will comply with all DCIS policies. The belt badge should not be worn when an agent is carrying a non-DCIS authorized weapon.

39.7. Accountability

39.7.a. **Transfer of Personnel.** Special agents and investigators authorized to carry DCIS badges and/or credentials shall retain them upon transfer to a new duty station within DCIS. The field office to which they are transferred shall assume inventory accountability for the DCIS badge and credentials.

39.7.b. **Retirement of Special Agents.** With the approval of the special agent's SAC, the credentials may be encased in a shadowbox and presented to the special agent upon retirement. Send credentials to HQ DCIS/04, which will forward them to the Office of Security. Both halves of the credentials will be permanently perforated with the word "Retired." The credentials will then be encased. The mounting of credentials in any other manner or for any other purpose is prohibited unless the specific written approval of the Assistant Inspector General for Investigations, Internal Operations, is obtained. A credential permanently perforated with the word "Retired" shall not be carried on the person. In accordance with IGDINST 1432.1, "Incentive and Honorary Awards Program," November 26, 2013, credentials will be forwarded to HCAS Awards Program

Coordinator for processing. The HCAS Awards Program Coordinator will secure the shadowbox and associated engraving.

39.7.c. Inventory

39.7.c.(1). Local field and Headquarters supervisors shall conduct annual inventories of badges and credentials. Ensure that each item is properly accounted for and forward the inventory to HQ DCIS/04. In accordance with IGDINST 5200.3, submit the annual inventory no later than **December 31**. HQ DCIS/04 will apprise the Office of Security in writing of the results of annual inventories.

39.7.c.(2). In addition to annual inventories, inspection teams shall check credentials, credential cases, badges, and badge carriers during all inspections of subordinate components. To the extent practicable, and where time and other factors permit, field office supervisors should also conduct such a check during visits to subordinate offices.

39.8. Loss of Badges and Credentials

39.8.a. In the event that badges or credentials are lost, or cannot be recovered from personnel who no longer require them or are no longer authorized to have them, the first-line supervisor shall immediately notify (within 24 hours), through the chain of command, the Deputy Assistant Inspector General for Investigations, Internal Operations (DAIGI/INT.) Initial notification may be by telephone, but shall be followed up with a memorandum detailing the circumstances of the loss, theft, etc. Within 3 days of any loss or theft of a law enforcement badge or credential, both the employee and the first line supervisor shall provide the OSEC and the Office of Quality Assurance and Standards, Internal Review Division (IRD) with memoranda detailing the loss or theft. The SAC or ASAC shall initiate a Financial Liability Investigation of Property Loss (DD Form 200, July 2009), and can be located at <http://www.dtic.mil/whw/directives/infomgt/forms/dd/ddforms0001-0499.htm>). Complete blocks 1, 3, 5, 6, 9, 10, and 11. Leave the remaining blocks blank. Forward the partially completed DD Form 200 to the DAIGI/INT for further review and action no later than 5 working days (10 working days for field elements) after discovering the loss, theft, etc.

39.8.b. If a special agent should discover his/her DCIS badge has been lost or stolen, it is the special agent's responsibility to notify the local police department in the immediate vicinity to request that a National Crime Information Center entry be made on his/her particular badge number. The un-numbered badge cannot be entered into NCIC.

39.8.c. If a special agent loses his/her badge and it is not recovered, the SAC or ASAC may request a replacement badge from HQ DCIS/04. The Deputy Inspector General for Investigations (DIG-INV) will approve or disapprove this request. In all cases involving a change of badge or credential number, make an appropriate entry to the Headquarters Personnel Data System.

39.8.d. If a special agent or investigator discovers his/her credentials have been lost or stolen and are not recovered within 15 calendar days, submit a written request for new permanent credentials. The justification of the request should indicate "loss." New special agent credentials will bear a credential number different from that of the lost credentials. If the lost credentials are

recovered later, forward them to the Office of Security through HQ DCIS/04 for record purposes and for destruction.

39.9. Recovery and Disposition

39.9.a. The supervisor will ensure the recovery of badges and credentials from personnel who no longer require them. In the event of unexpected hospitalization, prolonged illness, extended personal travel outside the country, internal inquiry or investigation, extended leave without pay status, or other situations where recovery of badge and credentials may be required, supervisors must recover badges and credentials and provide for their protection until the bearer returns to duty.

39.9.b. If the recovery of badges and credentials is permanent, disposition of recovered badges, credential cards, and cases shall be as follows.

39.9.b.(1). **Credential Cards.** Return to HQ DCIS/04 by FedEx, UPS, U.S. Postal Service, or other company with similar mail-tracking capability.

39.9.b.(2). **Badges.** Same as credential cards.

39.9.b.(3). **Credential Cases.** Local destruction is authorized when no longer serviceable.

39.9.c. The cognizant SAC/ASAC shall notify the DAIGI/INT, of the recovery of badges and credentials.

39.10.a. Retired Special Agent Identification Card. Issued to retired DCIS special agents in accordance with the guidelines in Attachment A and action memorandum for the Office of Security as shown in Attachment B. The card shows the name, signature, and photograph of the bearer, and the authorizing signature of the DoD Inspector General. The Retired Special Agent Identification Card will be used for personal identification in compliance with 18 U.S.C. §926C, “Law Enforcement Officers Safety Act of 2004 (LEOSA),” as amended and DoDI 5525.12.

ATTACHMENT A

**PROCEDURES FOR REQUESTING THE RETIRED SPECIAL AGENT
IDENTIFICATION CARD**

The following memorandum is a template for agents to request retired/separated ID cards. Requests must include a current digital photograph (1¼" x 1½"), personal mailing address and a telephone number and completion of the "signature page." The ID card will only be issued once the special agent has turned in the officially issued DCIS badge and credentials.

If the requesting agent separated from service but otherwise met the provisions of LEOSA, s/he will be eligible for the ID card. Therefore, the following memo should be written appropriately to reflect which situation the requesting individual meets.

Date

Internal Operations Directorate
Defense Criminal Investigative Service
4800 Mark Center Drive
Alexandria, VA 22350

I am writing to request a retired/separated Special Agent ID card based upon criteria. I would like my name to appear on the card as follows:

[Name as you would like it to appear]

My official retirement/separation date is/was _____.

I hereby certify that I meet the requirements of Section 926C of title 18, United States Code as outlined in paragraph E2.3, Enclosure 2 of DoDI 5525.12, and that I am not now prohibited from carrying a firearm.

I have enclosed a color digital photograph of myself to be used on the ID card. Please return the completed badge and ID card to me at the following address:

[Mailing Address]

I can be contacted by telephone at [telephone number].

Signature of Requester

Signature of Notary

ATTACHMENT B



(Investigations)

**INSPECTOR GENERAL
DEPARTMENT of DEFENSE**
4800 MARK CENTER DRIVE
ALEXANDRIA, VA 22350

ACTION MEMO

FOR: Office of Security

FROM: [Name],
Assistant Inspector General for Investigations – Internal Operations Directorate

THROUGH: [Name of Administrative Officer]

SUBJECT: Retired/Separated Special Agent (SA) Identification Card

Request the listed employee be issued a Retired/Separated Law Enforcement Officer (LEO) identification card as indicated.

Name on ID Card:

SSN:

Previous Job Title:

IG Component:

Justification: Individual retired/separated from DCIS as a LEO in good standing and has met the requirements of Section 926C of Title 18 U.S.C., as outlined in paragraph E2.3 of DoD Instruction 5525.12.

COORDINATION: None

CHAPTER 40

CYBER CRIMES PROGRAM

<u>Contents</u>	<u>Section</u>
General	40.1.
Policy	40.2.
Authority	40.3.
Selection of Cyber Crimes Agents	40.4.
Training and Professional Development	40.5.
Resources	40.6.
Computer Intrusion/Incident Referral Process	40.7.
Digital Media Acquisition and Examination	
Standard Operating Procedures	40.8.
Requesting Cyber Field Office Support	40.9.
Digital Media Considerations	40.10.
Reporting Requirements	40.11.
Quality Assurance Program	40.12.
Workload Analysis Metrics	40.13.

40.1. General

40.1.a. This chapter establishes policies and procedures for criminal investigations and other investigation-related support services, hereinafter referred to as cyber crimes, where the crime involves a form of digital media consisting of at least one computer, electronic data storage, network, communication device, or other form of digital media; and those collection, examination, analysis, and reporting activities undertaken by the Defense Criminal Investigative Service (DCIS), Department of Defense Inspector General (DoD IG). Cyber crimes may encompass offenses including, but not limited to:

- 40.1.a.(1). Intrusions, to include unauthorized access;
- 40.1.a.(2). Misuse;
- 40.1.a.(3). Denial to, or loss of integrity in, DoD data and systems;
- 40.1.a.(4). Compromise or exfiltration of Defense-critical technologies or intellectual property from DoD or cleared Defense contractor systems;
- 40.1.a.(5). Compromise or exploitation of DoD account data;
- 40.1.a.(6). Fraud in connection with DoD system maintenance and defense; and
- 40.1.a.(7). Child pornography offenses.

Digital media acquisition and examination is an investigative method used to identify and recover potential evidence that often plays a key role in DCIS investigations.

40.1.b. The DCIS Cyber Field Office provides investigative and digital media acquisition and examination support across the spectrum of DCIS investigations. While other field office personnel may open cyber crime cases, Cyber Field Office agents are trained and experienced to address the technical aspects of such investigations.

40.2. Policy

40.2.a. Cyber Crimes Investigations. DCIS will evaluate and document all cyber intrusions involving DoD and DoD-protected computers pursuant to Special Agents Manual (SAM) Chapter 28, “Investigative Reports.” DCIS may also investigate all criminal activity that adversely affects the DoD Global Information Grid (GIG), such as, but not limited to, denial of service, malware, and/or misuse of computer and communications resources. Title 18, United States Code, section 1030(e)(2), defines a protected computer.

A computer exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.

40.2.a.(1). DoD cyber incidents are grouped into categories based on severity. Attachment A lists these categories and the corresponding investigative response.

40.2.a.(2). DCIS may investigate child pornography offenses involving DoD computer systems or DoD personnel (military, civilian, or contractor). Incidents of adult pornography on DoD computer systems will be referred to the appropriate agency or component for administrative investigation.

40.2.b. Digital Media Examination. The seizing of digital media due to its potential evidentiary value and the resulting examination, analysis, and reporting will be conducted in accordance with guidance provided by this chapter, other applicable SAM chapters, and applicable statutory and regulatory requirements.

40.2.b.(1). Only a General Schedule (GS) series 1811 DCIS Cyber Crime Agent (CCA), a non-GS 1811 Cyber Crime Investigator (CCI), other DCIS personnel as authorized by the Cyber Field Office Special Agent in Charge (SAC), the Defense Computer Forensics Laboratory (DCFL), other Federal or regional law enforcement forensics laboratories, or other appropriately trained law enforcement personnel working jointly with DCIS will perform digital media acquisition, examination, and/or analysis in support of DCIS investigations. To ensure high standards and consistency of work product, DCIS agents should use DCIS CCAs or CCIs prior to seeking assistance from other law enforcement agencies; case agents must coordinate any non-Cyber Field Office assistance, to include using DCFL, with the servicing CCA. The Cyber Field Office SAC shall authorize any agreement for digital media support services with a non-governmental facility before any such work is performed. Without prior authorization from the Cyber Field Office SAC, CCAs/CCIs will not assist other law enforcement agencies in which DCIS is not a joint participant. DCIS agents will submit material for digital media examination or analysis to the DCFL through their servicing CCA and with the concurrence of the servicing Cyber Resident Agent in Charge (RAC).

40.2.b.(2). Whenever possible, only DCIS CCAs/CCIs, other DCIS special agents under the guidance of a DCIS CCA/CCI (either on site or telephonically), a qualified law enforcement officer from another agency, or members of a cyber incident response team shall seize digital evidence and maintain chain-of-custody. If an individual other than a CCA seizes digital evidence, the case agent should coordinate with their servicing CCA as soon as practical after the seizure.

40.3. Authority. SAM Chapter 1, “Organization, Mission, Jurisdiction, and Authorities,” sets forth the various legal authorities for DCIS to conduct investigations. The guidelines for acquiring and searching digital evidence generally derive from five authorities:

- 40.3.a. Search warrant.
- 40.3.b. Grand Jury subpoena.
- 40.3.c. Inspector General subpoena.
- 40.3.d. Consent search.
- 40.3.e. Administrative inquiry.

40.4. Selection of Cyber Crimes Agents

40.4.a. To guarantee a maximum return on the costs associated with specialized cyber crimes training, newly-appointed CCAs will sign a 3-year service agreement (Attachment B). CCAs who wish to discontinue serving in the Cyber Field Office at or after the conclusion of the 3-year period may make the request to Cyber Field Office RACs or SAC no less than 6 months in advance. The service agreement will be waived if a CCA is selected for a promotion opportunity within DCIS or resigns from DCIS to seek other Federal Government employment. All other requests to waive the service agreement must be adjudicated by the Deputy Inspector General for Investigations.

40.4.b. With regard to the personal honesty and integrity and the reporting of personal misconduct, all CCAs/CCIs are required to comply with IGDINST O-5200.2, “Personnel Security Program,” August 23, 2007, and DoD Regulation 5200.2-R, “Personnel Security Program,” Change 3, February 23, 1996.

40.5. Training and Professional Development

40.5.a. **Training.** Successful completion of applicable formal training in digital media acquisition and/or examination is required and must be completed before a CCA/CCI can perform any investigation-related digital media support work. The Defense Cyber Investigations Training Academy (DCITA) and Federal Law Enforcement Training Center (FLETC) are the preferred sources of formal digital media support/cyber crimes training. The Cyber Field Office SAC may approve other training sources as required to meet mission need. Each fiscal year, CCAs/CCIs are required to complete at least 20 hours of documented cyber crimes or digital media support training. Documentation must identify the source of training, course title, dates of training or completion date, and the number of training hours completed. The Cyber Field Office SAC, or designee, determines if a CCA/CCI training activity is acceptable towards the annual

minimum training requirement. CCAs/CCIs who fail to satisfy the training requirement will not be permitted to perform digital media support duties until the training requirement is met, or the requirement is waived in accordance with 40.5.b.(3).

40.5.b. Proficiency Requirements

40.5.b.(1). **Certification.** CCA/CCI certification is not mandatory, but is highly desirable for expert witness consideration, and as a means of documenting proficiency and completion of formal training. Potential certifications are:

40.5.b.(1).(a). Any applicable DCITA certification

40.5.b.(1).(b). International Society of Forensic Computer Examiners
Certified Computer Examiner

40.5.b.(1).(c). ISC² Certified Cyber Forensics Professional

40.5.b.(1).(d). GIAC Certified Forensic Analyst

40.5.b.(2). **Testing.** At least once every 3 years, CCAs/CCIs are required to pass a digital media acquisition and examination proficiency test issued by the Cyber Field Office. CCAs/CCIs who fail to satisfy the testing requirement will not be permitted to perform digital media support duties until successfully completing the proficiency test, or the requirement is waived in accordance with 40.5.b.(3).

40.5.b.(3). **Waiver.** If a CCA/CCI is unable to fulfill the proficiency requirement for certification or testing, the Cyber Field Office SAC may waive the proficiency requirement for up to 12 months in order to allow the CCA/CCI to meet the proficiency requirements. A waiver of more than 12 months can be granted by the Cyber Field Office SAC in the event the DoD IG cannot provide adequate budgetary support to permit a CCA/CCI to obtain training towards testing and certification. The Cyber Field Office SAC holds the authority to provide additional proficiency requirement waivers as required to meet the field office operational need.

40.5.b.(4). **Tracking.** The Digital Media Support Program will maintain an inventory of all Cyber Field Office CCAs/CCIs certification, test results, and/or proficiency requirement waivers.

40.5.c. **Allocation of Training Slots.** In order to maintain DCIS's digital media/cyber crimes standards and consistency of work product, the Cyber Field Office SAC must approve the attendance of any non-Cyber Field Office Personnel to attend any DCITA and/or FLETC computer crime/digital media support training.

40.6. Funding and Equipment

40.6.a. IG Instruction 5000.64, “Property Management Program,” August 23, 2013, establishes inventory requirements for accountable property. The Cyber Field Office administrative support assistant will normally function as the Cyber Field Office Property Custodian. The Cyber Field Office, in coordination with DoD IG ISD, is responsible for the budgeting, acquisition, and management of specialized computer, communications, and networking hardware and software. Except for the specialized hardware and software provided/funded by the Cyber Field Office, all other logistics support for CCAs/CCIs is provided through the DCIS office where the CCA/CCI is resident, DoD IG Information Systems Directorate (ISD), and the DoD IG Administration and Logistics Services Directorate (ALSD).

40.6.b. Specialized CCA/CCI hardware and software may not be embellished, converted to general office use, permanently reconfigured for other purposes, or removed from availability without the written approval of the Cyber Field Office SAC or designee. Connecting specialized CCA/CCI hardware or software to the DoD IG enterprise is prohibited, without coordination of the Cyber Field Office SAC or designee, and the written approval of the DoD IG Designated Accrediting Authority (DAA). The DoD IG DAA, as defined in DoD 8570.01-M, chapter 5, is the responsible party to accept all DoD IG Information Assurance risk.

40.7. Cyber Intrusion/Incident Referral Process

40.7.a. All cyber intrusion/incident alerts relating credible information that a crime has occurred or is about to occur will result in either a case initiation or information report, as appropriate. If a non-CCA DCIS agent initiates a cyber crime case or information report, he/she will notify the Cyber Field Office SAC as soon as practical.

40.7.b. In situations where a cyber crime, intrusion/incident crosses geographic boundaries, the CCA (or, if an investigation is opened by a non-CCA agent, the field office) with the greatest number of affected systems will assume the lead role in case initiation and management. Efficiency, resource, and other circumstances may require deviation from this general policy.

40.7.c. If an investigation discloses that a cyber crime, intrusion, or incident also affects systems within the jurisdiction of another law enforcement agency, the DCIS lead agent will promptly contact representatives from that agency.

40.8. Digital Media Acquisition and Examination Standard Operating Procedures (SOP).

40.8.a. In lieu of DCIS-specific digital media support SOPs, CCAs/CCIs will follow community best practices. These practices may be derived from, among other things, DOJ manuals, policy statements, or investigation-specific guidance provided by the Department of Justice (DOJ). These principles are intended to provide CCAs/CCIs with a general framework for conducting acquisition, examination, and analysis activities, and are not meant to constitute step-by-step checklists. CCAs/CCIs should address legal questions to an Assistant United States Attorney, DOJ’s CCIPS, or the DoD IG Office of General Counsel.

40.8.b. Digital Media Acquisition

40.8.b.(1) Digital media-based evidence will be seized in accordance with SAM Chapter 17, “Physical Evidence and the Crime Scene,” Chapter 18, “Evidence Custody System,” and Chapter 19, “Searches.” CCAs/CCIs will complete a Digital Media Acquisition Worksheet (Attachment C) and/or a Mobile Device Acquisition Worksheet (Attachment D) for each digital media item, in addition to any required Evidence Tags (DCIS Form 15) and Evidence Custody Documents (DCIS Form 14). In situations where DCIS is not the lead investigative agency, CCAs/CCIs may use the lead agency’s evidence custody documents in place of the DCIS Digital Media Acquisition Worksheet.

40.8.b.(2). Barring exigent circumstance, the acquisition of digital media will consist of collecting at least two copies of the original media, duplicated onto sanitized media, and in a manner to allow verification of the original media. Multiple verifiable copies help protect against duplicating media failure and the loss of potential evidence.

40.8.c. Digital Media Examination

40.8.c.(1). CCAs/CCIs will use Cyber Field Office approved digital media examination hardware and software in accordance with vendor-developed instructions. CCAs/CCIs will document all examination steps undertaken, tools used, and any resulting observations.

40.8.c.(2). Barring exigent circumstance, the examination of digital media will be conducted on a verified duplicate of the original media. If only one verified copy of the original media exists, the CCA/CCI will duplicate the verified copy onto sanitized media to create a duplicate working copy, verify the working copy, and use the working copy for any examination or analysis.

40.8.d. Use of Encryption.

40.8.d.(1). Digital media acquisition and examination will use a minimum of 128-bit Advanced Encryption Standard (AES) encryption to protect the confidentiality of the media contents during transportation between physical locations, to include but not limited to personal transport between work sites and offices, or shipping between physical locations. Encryption ensures reasonable confidentiality of the media’s contents and minimizes the data exposure risk that could harm the DoD, DoD IG, DCIS, and its business partners.

40.8.d.(2). If during the process of digital media acquisition or examination, a CCA/CCI determines a circumstance exists that will preclude the use of encryption, the CCA/CCI will use an alternate pre-approved method to complete the mission. The CCA/CCI will inform the Cyber Field Office SAC or designee of the circumstance that precluded the application of encryption.

40.8.e. Digital Media Support Hardware and Software. The Digital Media Support Program will develop and distribute a standard hardware software build for DCIS digital media acquisition and examination platforms. The standard hardware and software will include utilities that are in wide use by the digital media examination community and that have passed testing by the DCFL, National Institute of Standards and Technology (NIST), DCIS, or similar organizations. CCAs/CCIs may test new utilities to determine suitability to support a case, but must not rely on a non-approved utility to produce any work product in support of an active case. If the standard build does not meet mission needs of the Cyber Field Office, other utilities must be submitted to the Cyber Field Office SAC or designee for approval.

40.9. Requesting Cyber Field Office Support

40.9.a. Whenever DCIS special agents anticipate a search warrant, consent search, or other investigative activity involving computers, networks, digital media, or other electronic equipment, the case agent must coordinate with their respective Cyber Field Office RAC as early as possible. The Cyber Field Office RAC will assign a CCA to provide the case agent with a digital media case assessment. The case agent must work closely with the CCA to plan for any computers, networks, digital media, or other electronic devices that might be encountered throughout the case. Upon the case assessment, the case agent requiring Cyber Field Office assistance, will complete, and forward a Lead Request Form 1 through the appropriate chains of command. This preparatory work is necessary to enable the case agent to properly draft a search warrant affidavit (if applicable) and to allow the CCA to assemble the requisite resources. With few exceptions, the completion of the Lead Request Form must be accomplished prior to a search warrant operation (See Attachment E for a sample Pre-Search Warrant Request) or after the non-CCA seizure of digital media (See Attachment F for a sample Computer Forensics Analysis Request).

40.9.b. The appropriate Cyber Field Office RAC coordinates with CCAs/CCIs, participating investigative agencies, and the Cyber Field Office SAC to arrange for adequate personnel, funding, and other resources to support the anticipated need. DCIS case agents and field management must coordinate with Cyber Field Office management prior to offering and/or committing Cyber Field Office resources.

40.9.c. After the acquisition of digital media, the case agent requiring Cyber Field Office digital media examination and analysis support will complete, documenting in as much detail as possible, and forward a Lead Request Form 1 to the CCA/CCI for the support requested through the appropriate chains of command.

40.9.d. All outcomes of a Lead Response Form 1 for digital media acquisition, examination, or analysis support will be provided to the case agent on a Lead Response/ Digital Media Acquisition Form 1 from the supporting CCA/CCI, reviewed and approved by the appropriate Cyber Field Office manager.

40.10. Digital Media Considerations

40.10.a. To ensure a thorough, expeditious, and legally sufficient digital media acquisition, examination, and analysis, the case agent is responsible for providing the CCA/CCI with as much guidance as possible about the nature of the case, information expected to be contained within the digital media, a copy of the search authority (warrant, consent, warning banner), and any other information relevant to the investigation.

40.10.b. Whenever possible and with the guidance of the servicing CCA/CCI, the case agent or other investigative support personnel may conduct non-technical digital media review tasks associated with their digital evidence, such as document searches and review. The servicing CCA/CCI will process the digital media, perform any technical processes, and facilitate the case agent's review process using an appropriate media that can be used to identify and locate potential evidence, such as documents, key words, graphics, files, and other information relevant to the investigation.

40.10.c. When circumstances require the servicing CCA to submit digital media on behalf of the case agent to the DCFL or another law enforcement forensics laboratory, the CCA will advise the case agent as soon as possible, and keep the case agent apprised of the status of the externally-sourced work.

40.11. Reporting Requirements

40.11.a. Once the CCA/CCI completes digital media acquisition, examination, or analysis support, he/she will prepare a Lead Response/Media Analysis Report or Lead Response/Digital Media Collection Form 1 documenting the findings. This Form 1 will follow a standard format (See Attachments G and H for samples) and contain a minimum of:

- 40.11.a.(1). Identify of the reporting organization,
- 40.11.a.(2). Case identifier or other tracking number,
- 40.11.a.(3). Identity of the examination requester,
- 40.11.a.(4). Relevant dates of work, to include the report date,
- 40.11.a.(5). Descriptive list of the evidence examined,
- 40.11.a.(6). Examination requested,
- 40.11.a.(7). General description of the examination,
- 40.11.a.(8). Results, conclusions, and derived items,
- 40.11.a.(9). Name and signature of the CCA/CCI or other examiner

40.11.b. If an analysis utility generates a separate report, that report can be attached to the Form 1 or provided to the case agent on an appropriate media, such as a CD or DVD.

40.11.c. If the CCA/CCI produces evidentiary files during the digital media examination/analysis, he/she will provide these to the case agent on an appropriate media, such as CD/DVD or other externally-connected digital media device.

40.11.d. The insertion or connection of any media, such as a CD, DVD, or other externally-connected digital media device provided by the CCA/CCI to the case agent comes with serious potential risks to the investigation and, DoD computers and networks. Before any provided media or device is connected to an ISD-issued computer or other network-connected computer, the case agent should consult the servicing CCA, and follow all ISD policies and procedures related to the use of externally-provided media in ISD-issued computers. Risks include, but are not limited to, execution of malware, compromise of DoD computers and networks, sending of unsent electronic mail messages, and exposing non-DCIS personnel to contraband.

40.12. Quality Assurance Program

40.12.a. CCAs/CCIs and the Cyber Field Office leadership play a central role in administering a quality assurance (QA) program that covers all aspects of digital media support from acquisition, through examination, to production of potential evidence. A comprehensive and proactive QA program maintains consistency and high standards of work product.

40.12.b. Unless otherwise waived, all CCAs/CCIs will maintain technical proficiency.

40.12.c. All Digital Media Analysis Report Forms 1 will be 100 percent administratively reviewed by the CCA/CCI's immediate supervisor.

40.12.d. At least 10 percent of all Digital Media Analysis Report Forms 1 will be reviewed for technical sufficiency and reporting compliance by another CCA/CCI or Cyber Field Office manager who maintains current technical proficiency, as designated by the CCA/CCI's immediate supervisor.

40.12.e. The QA program, described in 40.12.a through 40.12.d, will be reviewed at least once every 3 years to ensure the QA needs are sufficient.

40.13. Workload Analysis Metrics

40.13.a. Unless otherwise waived by the Cyber Field Office SAC, RAC, or Program Director, CCAs/CCIs will complete all assigned lead requests within 90 days of the date of the lead request. A lead request is considered closed when the Lead Response Form 1 has been generated and submitted for administrative review.

40.13.b. Within 3 business days of the completion of the investigative documentation, CCAs/CCIs or the supervising RAC will enter digital media support work efforts related to

digital media acquisition, examination, production, and other electronic evidence related statistics into a Cyber Field Office SAC approved database in order to facilitate Cyber Field Office statistical reporting to senior leadership and to facilitate proficiency requirement compliance.

ATTACHMENTS

- A Cyber Incident Category Levels
- B Cyber Crimes Agent Service Agreement
- C Digital Media Acquisition Worksheet
- D Mobile Device Acquisition Worksheet
- E Example of a Lead Request Form 1 (pre-search)
- F Example of a Lead Request Form 1 (post-search)
- G Example of a Lead Response/Media Analysis Report Form 1
- H Example of a Lead Response/Digital Data Collection Form 1

ATTACHMENT A

CYBER INCIDENT CATEGORY LEVELS

Category	General Description	Investigative Action
I	Full Root Access	(b)(7)(E)
II	User Level and Web Page Hacks	
III	Attempted Access	
IV	Denial of Service	
V	Poor Security Practice	
VI	Probes/Scans	
VII	Malicious Logic (Virus/Worm)	

* Subject to Cyber Field Office SAC guidance based upon prevailing MCIO counterintelligence initiatives.

ATTACHMENT B

CYBER CRIMES AGENT SERVICE AGREEMENT



**INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
DEFENSE CRIMINAL INVESTIGATIVE SERVICE**

Cyber Crimes Agent Service Agreement

In recognition of the resources and time associated with specialized the specialized training and agency resource commitment, I agree to serve as a Cyber Crimes Agent (CCA) for a minimum of 3 years from the date of my appointment. I will provide the Cyber Field Office SAC with at least 6-month notice if I plan to discontinue CCA duties at or after the completion of this 3-year period. I understand that this service agreement will not restrict me from applying for promotion opportunities within DCIS or resigning from DCIS to seek other Federal Government employment. I further understand that any other request to waive the service agreement must be adjudicated by the Deputy Inspector General for Investigations.

Cyber Crimes Agent

Signature

Cyber Field Office RAC

Signature


Cyber Field Office SAC

Signature

Agreement Effective Date


ATTACHMENT C

DIGITAL MEDIA ACQUISITION WORKSHEET

 INSPECTOR GENERAL DEPARTMENT OF DEFENSE DEFENSE CRIMINAL INVESTIGATIVE SERVICE			
Digital Media Acquisition Worksheet			
I. General Information			
UID	Case Name	Computer Crimes Agent/Investigator	Date
II. Location Information			
Address/Room/Location in Room			
III. Source Media to be Acquired			
Make	Model Number	Serial/Property Number or other Identification	
Status <input type="checkbox"/> On <input type="checkbox"/> Off <input type="checkbox"/> Locked <input type="checkbox"/> Confirmed encrypted	Description	System Date/Time	Actual Date/Time
IV. Source Media Imaging Information			
<i>Source Item 1</i>			
Manufacturer	Model Number/Description	Capacity	Serial Number
Imaging Format (.e01, dd)	Image Name	Verification/Hash Value	
Notes			
<i>Source Item 2</i>			
Manufacturer	Model Number/Description	Capacity	Serial Number
Imaging Method	Image Name	Verification/Hash Value	
Notes			
V. Destination Media Information			
Manufacturer	Model Number	Capacity	Serial Number
Manufacturer	Model Number	Capacity	Serial Number
Additional Notes <i>Continue your notes on the other side of the worksheet, if needed</i>			

ATTACHMENT D

MOBILE DEVICE ACQUISITION WORKSHEET

 INSPECTOR GENERAL DEPARTMENT OF DEFENSE DEFENSE CRIMINAL INVESTIGATIVE SERVICE				
Mobile Device Acquisition Worksheet				
I. General Information				
UID	Case Name	Computer Crimes Agent/Investigator	Date	
II. Location Information				
Address/Room/Location in Room/End user				
III. Mobile Device(s) to be Acquired				
Device 1				
Type	Make		Model	
Serial Number	IMEI/MEID		SIM Card Number	
Status <input type="checkbox"/> On <input type="checkbox"/> Off <input type="checkbox"/> Locked	Airplane Mode <input type="checkbox"/> On <input type="checkbox"/> Off <input type="checkbox"/> Unknown	WiFi <input type="checkbox"/> On <input type="checkbox"/> Off <input type="checkbox"/> Unknown	Bluetooth <input type="checkbox"/> On <input type="checkbox"/> Off <input type="checkbox"/> Unknown	Imaging Method/Tool
Imaging Format	Image Name		Verification/Hash Value	
Notes				
Device 2				
Type	Make		Model	
Serial Number	IMEI/MEID		SIM Card Number	
Status <input type="checkbox"/> On <input type="checkbox"/> Off <input type="checkbox"/> Locked	Airplane Mode <input type="checkbox"/> On <input type="checkbox"/> Off <input type="checkbox"/> Unknown	WiFi <input type="checkbox"/> On <input type="checkbox"/> Off <input type="checkbox"/> Unknown	Bluetooth <input type="checkbox"/> On <input type="checkbox"/> Off <input type="checkbox"/> Unknown	Imaging Method/Tool
Imaging Format (.e01, dd)	Image Name		Verification/Hash Value	
Notes				
IV. Destination Media Information				
Manufacturer	Model Number	Capacity	Serial Number	
Manufacturer	Model Number	Capacity	Serial Number	
Additional Notes <i>Continue your notes on the other side of the worksheet, if needed</i>				

CHAPTER 41

TRAINING

<u>Contents</u>	<u>Section</u>
General	41.1.
Policy	41.2.
Law Enforcement Training	41.3.
Specialized Programs	41.4.
Asset Forfeiture Continuing Education Seminar	41.5.
On-the-Job Training Program	41.6.
Leadership and Supervisory Training	41.7.
Executive Training	41.8.
Non-Law Enforcement Training	41.9.
Administrative Support Training	41.10.
Non-Critical Training	41.11.
Conferences and Seminars	41.12.
Procedures	41.13.
Travel Procedures	41.14.

41.1. General

41.1.a. This chapter contains policies and procedures for achieving effective employee development objectives for employees of the Defense Criminal Investigative Service (DCIS), Office of the Deputy Inspector General for Investigations (ODIG INV), Department of Defense, Office of the Inspector General (DoD OIG).

41.1.b. DCIS recognizes that employee development is a principal means for building and maintaining a permanent cadre of criminal investigators, leaders, and administrative personnel skilled in the performance of their official duties and cognizant of the latest management, scientific, professional, and technical developments. Skilled personnel will promote efficiency, economy, and effectiveness in Agency operations.

41.1.c. DCIS will provide training and development to meet job requirements for all employees without discrimination because of age, race, religion, color, national origin, politics, or gender.

41.1.d. Available training resources within DoD OIG will be used as practicable. In addition, appropriate use will be made of DoD, interagency, and non-Government facilities, in that order.

41.1.e. The policies and procedures contained in this chapter are consistent with DoD Instruction 1430.02, "Civilian Career Management," April 6, 2006.

41.1.f. The DCIS Training Academy, which is part of the Internal Operations Directorate, is comprised of a Director for Training (Dir-TR), four Program Managers: Use of Force Program Manager (UoF PM), Program Manager – Advanced Programs (PM-AP), Program Manager – Basic Programs (PM-BP), and Program Manager – Training Accreditation (PM-TA); a Firearms Inventory Control Manager (FICM); one Administrative Support Assistant (ASA); and the DCIS Headquarters (HQ) Training Coordinator. These employees are hereafter referred to as the DCIS Training Staff.

41.1.g. The DCIS Training Staff is responsible for the effective design, development, implementation, coordination, and management of DCIS training programs and for identifying training needs and resources within the Federal Government, as well as from private sources. In addition, the DCIS Training Coordinator is responsible for processing DCIS training requests and tracking the training budget. The DCIS Training Staff is located at the Federal Law Enforcement Training Center (FLETC), Glynco, GA.

41.2. Policy

41.2.a. All training requests, with the exception of OIG in-house courses (e.g., New Employee Orientation (NEO)), **must** be submitted on an OPM Standard Form (SF)-182 at least 6 weeks before the start of training. Employees are responsible for submitting the SF-182 through their chain-of-command to the DCIS Training Coordinator. The DCIS Training Coordinator or a staff member will notify the student when training has been approved and funded. Funding **must** be approved prior to attendance. Otherwise, failure to comply with this requirement could result in the employee being held responsible for training costs and any related travel expenses incurred.

41.2.b. All DCIS employees will receive training whenever necessary to enable them to perform the duties required by their position descriptions, as well as areas identified by senior leadership in the DCIS annual priority goals and objectives.

41.2.c. Supervisory managers, through coordination with their cognizant field training officers, will forward training recommendations to the DCIS Training Staff. The DCIS Training Staff will evaluate the requests, research training alternatives, and provide recommendations to the senior leaders or field training officers for implementation.

41.2.d. All supervisors and managers will receive training periodically to enable them to effectively supervise subordinates and/or manage resources and programs. During the annual year-end evaluation, senior managers will examine their employees' training histories to ensure all managers/developing leaders are receiving appropriate training.

41.2.e. When notified by the DoD OIG Learning Office Directorate (LOD), all employees will prepare and discuss with their supervisor an annual Individual Development Plan (IDP) (see Attachment A) in accordance with IG Policy Memorandum 2004-10, dated March 17, 2004. This IDP should be the basis for planning developmental training and is required for all DCIS employees. The IDP will be completed annually and updated in the Defense Automated Management Information System (DAMIS) by the individual employee. The employee's

supervisor will baseline (approve/disapprove) requested training opportunities in DAMIS after discussion. The information input into DAMIS is utilized by the OIG LOD for future budgetary calculations. ***Submission of an IDP is not a request for training. Only an approved SF-182 (referenced in paragraph 41.2.a.) submitted to the DCIS Training Coordinator, through the first-line supervisor, is considered an approved training request.*** The employee should maintain a copy of his/her IDP. A copy of the IDP will also be placed in the employee's office personnel file (not the HQ file) and a copy should be forwarded to the cognizant field training officer. Employees should use the course library maintained in DAMIS to identify courses to enhance his/her skills.

41.2.f. Each employee or the cognizant field training officer, as designated by each field office, shall be responsible for submitting a completed SF-182 in DAMIS for ***every*** training course approved by their first-line supervisor (with the exception of OIG in-house-delivered training). Training cannot be scheduled until an SF-182 is received by the DCIS Training Coordinator. Training request procedures are set forth in Attachment B. Contact the DCIS Training Coordinator if questions for this process arise.

41.2.g. Critical training (e.g., refresher training to maintain currency in certifications, training to meet Attorney General guidelines and Council of the Inspectors General on Integrity and Efficiency (CIGIE) guidelines, such as legal, investigative/administrative skills training, and supervisory/management training) will always receive priority consideration over noncritical training.

41.2.h. Office of Quality Assurance and Standards (QAS) verification inspections of the HQ directorates and field offices will include a review of the On-the-Job training program (OJT) and every employee's training history to determine whether employees are being scheduled for appropriate training opportunities.

41.2.i. Within the first 90 days of appointment, all DoD OIG employees are required to attend New Employee Orientation (NEO). NEO training is offered via VTC to field elements, but can also be attended in person at OIG Headquarters (Mark Center, Alexandria, VA). The Deputy Inspector General for Investigations (DIG INV) may waive an employee from the course based on prior DoD OIG experience. The LOD will notify the new employee's management when an employee has been scheduled to attend NEO.

41.3. Law Enforcement Training

41.3.a. **Required Training.** Within the first 18 months of appointment, all criminal investigators are required to attend "core" training, including the Criminal Investigator Training Program (CITP) and the DCIS Special Agent Basic Training (SABT) Program at FLETC.

41.3.a.(1). **FLETC Criminal Investigator Training Program (CITP).** Attendance is mandatory and should be scheduled as soon as possible after appointment. Prior graduation from an equivalent basic training program (e.g., the Federal Bureau of Investigation Academy, the Air Force Office of Special Investigations Academy, or the U.S. Army Criminal Investigative Division Command Basic Agents Course) is sufficient to meet this requirement.

41.3.a.(2). **DCIS Special Agent Basic Training (SABT) Program.** All newly hired special agents (GS-1811) at the GS-14 level and below are required to attend the SABT Program provided by the DCIS Training Staff at FLETC, Glynco, GA. Special agents are required to have completed SABT prior to deploying to a non-permissive environment. Exceptions to this policy will be granted only by the Assistant Inspector General for Investigations (AIGI), Internal Operations Directorate (INT) or the DIG INV in consultation with the AIGI, International Operations Directorate (INTL). Exceptions will be made in a written memorandum, which will be stored electronically on the International Deployment SharePoint site with the special agent's deployment application.

41.3.b. **DCIS Special Agent Refresher Training Program (SARTP).** The SARTP was developed to fulfill mandatory training requirements and provide training to enhance DCIS agents' ability to perform their mission. The primary training objectives are to meet the CIGIE requirement for continuing legal education, meet DoD requirements for emergency vehicle operations, enhance and standardize agents' use of force skills, and provide updated instruction in white collar investigative techniques. All agents at the GS-14 and below level must attend the SARTP no less than every 3 years.

41.3.c. **Deployment Readiness Program (DRP).** Prior to deploying to a non-permissive environment, special agents are required to have completed the DCIS DRP at FLETC, Glynco, GA. The DRP certification is valid for 24 months. Whether an agent does or does not deploy during that 24 months is immaterial. DRP will be completed again as a refresher after the 24-month expiration, and before an agent may deploy again. In cases where there is a scheduling conflict or unavailable seats in the DRP, completion of other U.S. Government-sponsored deployment training will be considered on a case-by-case basis. Exceptions to this requirement will only be made by the AIGI, INTL or the DIG INV. Exceptions will be made in a written memorandum, which will be stored electronically on the International Deployment SharePoint site with the special agent's deployment application.

41.3.d. **General Law Enforcement Training.** Law enforcement training at FLETC, the IG Criminal Investigator Academy (IGCIA), and the Defense Cyber Investigations Training Academy (DCITA) is available to criminal investigators. Although the FLETC curriculum may change slightly from time to time, the below listed training programs are generally unchanged. With supervisory approval and submission of an SF-182, attendance can be scheduled through the DCIS Training Coordinator based on published schedules, availability of space, and needs of the individual DCIS office. All FLETC and IGCIA courses must be cancelled at least 10 days prior to the start of the class or a replacement must be found by the field office to prevent DCIS from incurring tuition costs. Listed below are many of the pertinent courses offered at FLETC/IGCIA; however, this list is not exhaustive.

41.3.d.(1). **General Courses Offered at FLETC**

Advanced Interviewing for Law Enforcement Investigators Training Program
Case Organization and Presentation Training Program
Economic Crimes Investigation and Analysis
Financial Forensic Techniques Training Program

Grant Fraud Investigations Training Program
International Banking and Money Laundering Training Program
Internet Investigations Training Program
Money Laundering and Asset Forfeiture Training Program
National Suspension and Debarment Training Program
Procurement Fraud Investigative Training Program
Product Substitution Investigative Training Program

41.3.d.(2). Inspector General CIA Courses (export only)

IG Advanced Interviewing for IG Investigators
IG Public Corruption Investigations Training Program
IG Undercover Investigations Training Program
IG Undercover Operations for OIG Managers

41.3.d.(3). Specialized Courses

Computer Network Investigations Training Program
Covert Electronic Surveillance Training Program
Covert Electronic Tracking Program
Digital Evidence Acquisition Specialist Training Program
Digital Photography for Law Enforcement Level 1, 2
Field Training Evaluation Program
Firearms Instructor Training Program
Intelligence Analyst Training Program (Analysts: priority)
Internet Protocol Camera Training Program
Law Enforcement Control Tactics
Law Enforcement Fitness Coordinator Training Program
Law Enforcement Adjunct Instructor Training Program
Reactive Shooting Instructor Training Program
Recovery of Evidence from CCTV Video Recordings
Use of Force Instructor Training Program

FLETC, IGCIA, and DCITA catalogs and Web sites ((www.fletc.gov), (www.ignet.gov/igcia/index.htm), (www.dcita.edu/courses.html), respectively) contain specific details concerning each program and are accessible to all offices through their Internet Web pages. In addition, FLETC, IGCIA, and DCITA schedules are published by the DCIS Training Staff on the OIG shared drive at S:\DCIS\Training Program\Training Programs & Information\Training 2014 (or the current fiscal year). The Dir-TR will monitor and evaluate FLETC, DCITA, and IGCIA course offerings. On a scheduled annual basis, the Dir-TR will notify the field training coordinators and supervisors when the new FY training programs are published and ready for sign-up. Employees who requested the courses during the data call prior to publishing of the schedule will be annotated on the schedule. These employees will have first right of refusal; however, this does not preclude other employees from obtaining a seat in a course that they did not request during a prior data call. In this case, the employee must request a seat through their chain-of-command to the DCIS Training Coordinator or Training Program

Managers for a specific course date. The DCIS Training Coordinator will manage scheduling requests among the requestors.

41.3.e. Other Law Enforcement Training. Other law enforcement training is available from Federal agencies, law enforcement organizations, and various private vendors. Special agents and supervisors are encouraged to take advantage of such training whenever available, appropriate, and consistent with budgetary constraints. FLETC/IGCIA/DCITA law enforcement training will always take precedence over non-FLETC/IGCIA/DCITA law enforcement training in a given subject matter.

41.3.f. Other Sources of Training. Supervisors are encouraged to identify other sources of training, both regional and national, and report these proposed training sources through their field training officer and Special Agent in Charge (SAC) to the DCIS Training Staff. Web site and organizational information should also be forwarded for assistance with research.

41.3.g. Other Agencies. The DCIS Training Staff will coordinate with training representatives from other law enforcement agencies with similar missions, as well as non-law enforcement agencies, to explore available training opportunities for special agents, GS-1801s, analysts, and administrative personnel. The DCIS Training Staff will inform the field training officers of these findings.

41.4. Specialized Programs. Individuals selected for the below specialized programs should be interested in the programs and willing to be assigned to these positions for a reasonable period of time. The DCIS Training Staff will seek annual input from the requisite Program Manager of the specialized programs in order to assess the need for additional training or conferences.

41.4.a. Firearms Instructor Program

41.4.a.(1). Each SAC will appoint one Field Office Firearms Coordinator (FOFC) and sufficient additional firearm instructors to adequately conduct field office firearms training. The FOFC will be responsible for implementing the program throughout the field office. The DCIS UoF PM will provide program oversight for all firearms coordinators/instructors.

41.4.a.(2). Special agents designated as firearms instructors will attend the Firearms Instructor Training Program (FITP) at FLETC. Prior to attending the class, the designee must adequately practice and must be able to achieve a minimum score of 85 percent on the FLETC course of fire. Above average shooting skills are required to successfully complete this course. Students will be tested once on Day 1. If a minimum score of 85 percent is not achieved, students will be removed from the course and sent back to their duty station. Preparation is paramount. In addition, the firearms instructors will maintain current certification in cardiopulmonary resuscitation (CPR) and basic first aid. Dependent upon budget and course availability, it is recommended that firearm instructors will maintain proficiency and expertise in firearms training by attending a FLETC-sanctioned refresher training course every 5 years. The UoF PM may approve firearms instructors to, instead, attend an advanced course, such as one of

the following, in lieu of the Firearms Instructor Refresher Training Program (FIRTP). All firearms instructor training shall be coordinated through the UoF PM.

Reactive Shooter Instructor Training Program
Law Enforcement Rifle Training Program
Survival Shooting Training Program
Instructor Techniques for Non-Lethal Training Ammunition
Active Shooter Threat Instructor Training Program

41.4.b. Control Tactics Program

41.4.b.(1). Each SAC will appoint one Field Office Control Tactics Coordinator (FOCTC) and sufficient additional CT instructors to adequately conduct field office CT training. The FOCTC will be responsible for implementing the program throughout the field office. The DCIS UoF PM will provide program oversight for all CT coordinators/instructors.

41.4.b.(2). CT instructors will attend the Law Enforcement Control Tactics Instructor Training Program (LECTITP) at FLETC. Special agents designated as CT instructors must be medically cleared and able to complete all components of the DCIS Physical Readiness Test (PRT) at the “Fair” assessment level or higher. Requirements for successfully completing this course include intensive hands-on physical training lasting up to 8 hours a day and scenario-based training requiring the special agent to be contaminated with oleoresin capsicum (OC) spray. Further details on the LECTITP can be found at www.fletc.gov/ptd. In addition, all CT instructors will maintain current certification in CPR and basic first aid. Dependent upon budget and course availability, it is recommended that instructors will maintain proficiency and expertise in law enforcement control tactics by attending a FLETC-sanctioned refresher course every 5 years. All CT training will be coordinated through the UoF PM.

41.4.c. Health and Wellness Program

41.4.c.(1). Each SAC will appoint one Field Office Health and Wellness Coordinator (HWC) and sufficient additional Health and Wellness instructors to adequately conduct field office Health and Wellness training and physical readiness testing. The HWC will be responsible for implementing the program throughout the field office. The PM-Basic Programs (PM-BP) is responsible for the Health and Wellness program through the DCIS Training Academy and will provide program oversight for all Health and Wellness instructors.

41.4.c.(2). Health and Wellness instructors will attend the Law Enforcement Fitness Coordinator Training Program (LEFCTP) at FLETC. Prior graduation from an equivalent training program approved by the PM-BP (e.g., The Cooper Institute Law Enforcement Fitness Specialist training) may be sufficient to meet this requirement. Special agents designated as Health and Wellness instructors must have an interest in health and wellness and have no long-term disability that would prevent the instructor from participating in all components of the DCIS PRT. Prior to attending LEFCTP, the special agent must be able to pass the FLETC Physical Efficiency Battery (PEB) at the 40 percent or higher level. Details of the FLETC PEB can be found at: <http://www.fletc.gov/training/programs/physical-techniques->

[division/requirement-documents/physical-efficiency-battery-peb.html](#). Health and Wellness instructors will also maintain current certification in CPR and basic first aid. Bound by fiduciary controls and course availability, it is recommended that instructors will maintain proficiency and expertise in physical fitness by attending a FLETC-sanctioned refresher course every 5 years. All health and wellness training, to include DCIS PRTs, agency-required physicals, and fit for duty issues will be coordinated through the PM-BP.

41.4.d. Bloodborne Pathogens/Tuberculosis Program

41.4.d.(1). Each SAC will appoint one field office Bloodborne Pathogens (BBP)/Tuberculosis (TB) Instructor. The instructor will be responsible for implementing the program throughout the field office and ensuring that all special agents complete their mandatory Inspector General Electronic Learning (IGEL) system BBP/TB training on an annual basis. The PM-BP (Health & Wellness responsibilities) will provide program oversight for all instructors.

41.4.d.(2). Special agents designated as BBP/TB instructors will complete a train-the-trainer session approved or conducted by the Federal Occupational Health (FOH) infectious disease control consultant. In addition, instructors will receive yearly refresher training as directed by the PM-BP.

41.4.e. Technical Support Specialists

41.4.e.(1). Each SAC will appoint one primary Technical Support Specialist (TSS) and an alternate TSS to provide support assistance to the DCIS technical services program managed by DCIS HQ.

41.4.e.(2). Special agents designated as a TSS will attend the Covert Electronic Surveillance Program (CESP), formerly known as the Technical Investigative Equipment Training Program (TIETP), the Covert Electronic Tracking Program (CETP), and the Digital Photography for Law Enforcement Training Program II (DPLE2) at FLETC. This training and any advanced training will be coordinated through the Program Manager-Technical Services (PM-TS), Special Operations, located in Alexandria, VA. Other special agents may attend this training; however, the field TSSs will have priority placement. Training must be coordinated with the PM-TS and approved by the agent's first-line supervisor. PM-TS will coordinate with the DCIS Training Coordinator to obtain seats in these courses.

41.4.f. **Cyber Crimes Program.** Refer to SAM Chapter 40, "Computer Crimes Program," for current training requirements.

41.5. Asset Forfeiture Continuing Education Seminar. The Asset Forfeiture/Continuing Education Seminar (AF/CES) is managed by the DCIS Asset Forfeiture Program Manager and collaborated with the DCIS Training Academy. It shall be deployed to field agents every few years as needed and as budget dictates. The purpose of the AF/CES is to ensure that DCIS criminal investigators and other field personnel have the skills, knowledge, and resources to understand when and how to implement asset forfeiture techniques on DoD investigations. The Asset Forfeiture Program is a nationwide law enforcement initiative that deters crime by

depriving wrongdoers and criminal organizations of the proceeds of their crimes. Additional subject matters to be covered include Agency priorities and policy updates, leadership directives, current trends, best practices, and refresher training in investigative priority fraud matters.

41.6. On-the-Job Training Program. All newly employed DCIS agents will participate in the DCIS OJT program in conjunction with, and following completion of, all required core criminal investigator basic training programs. The requirements to complete this program are dependent upon the agent's background, work experience, and training history. Each supervisor will tailor the use of this OJT program to best benefit the needs of DCIS, as well as the abilities of the new special agent.

41.7. Leadership and Supervisory Training

41.7.a. Newly Assigned and Incumbent Supervisors. In order to comply with Title 5 C.F.R. Part 412 "Supervisory, Management, and Executive Development" and the FY 2010 National Defense Authorization Act, Section 1113, the OIG requires all newly assigned first-line supervisors to complete mandatory supervisor training within their first year of appointment. Additionally, incumbent supervisors are required to receive refresher training every 3 years. The Learning Planning and Organizational Development Division (LPODD), LOD, is responsible for developing or identifying training that meets these requirements. Generally, these programs will be conducted by the Office of Personnel Management (OPM) or The Graduate School USA. The LPODD will announce course dates and times on the OIG intranet Home page and by email. ***An SF-182 request is not required to be submitted to the DCIS Training Coordinator for these OIG in-house courses.*** DCIS supervisors must nominate a candidate by sending an e-mail request through their chain-of-command to the requisite course training specialist in LPODD.

41.7.b. Other Formal Training. Dependent upon budget and course availability, formal supervisory and management training is also available, as follows.

41.7.b.(1). FLETC Leadership and International Capacity Building Division (LICBD) offers law enforcement leadership and management training. The FLETC Web site (www.fletc.gov) provides a description of all leadership and management courses offered. Courses offered are:

- Law Enforcement Supervisor Leadership Training Program
- Law Enforcement Manager Training Program
- Situational Leadership® II for Law Enforcement Training Program
- Leadership through Understanding Human Behavior Training Program
- Women in Law Enforcement Leadership Training Program

41.7.b.(2). IGEL Online Training is available on the OIG intranet Home page. All OIG personnel have access to any online training course. Many supervisory and leadership courses are offered and can be completed at the leisure of the requestor. A record of completed courses is maintained on the "My Progress" tab for OIG personnel. In order to have an individual's record of completion documented in DAMIS, a completed SF-182 must be

submitted to denote “planned” status. An electronic copy of the completion certificate must then be uploaded in DAMIS to close out the individual training denoting “completed” status.

41.7.b.(3). Requests for supervisory and management training from private vendors must contain justification that explains why Federal Government sources are not available or are not appropriate for the training sought. A memorandum request should be forwarded (at least 6 weeks prior to commencement of training) to the Dir-TR with stated justification and concurrence from the cognizant SAC. Once approved, an SF-182 must be properly filled out and submitted to the DCIS Training Coordinator. Any registration forms required by the private vendor must also be submitted with the SF-182. Training request procedures are set forth in Attachment B.

41.8. Executive Training. Senior-level managers can be selected to attend executive training seminars at such institutions as the Federal Executive Institute. LPODD will announce various training courses as they become available. These courses are announced competitively. All applications are reviewed and ranked by an executive OIG Board consisting of the Deputy Inspectors General from each component. Final selection is made by the Inspector General.

41.9. Non-Law Enforcement Training. Other training is available as follows:

41.9.a. **In-House Courses by DoD OIG.** Due to the short duration of these programs, most are generally offered to Washington, D.C., metropolitan area employees only. Class offerings are listed on the intranet at the LPODD home page. In addition, the DCIS Training Staff announces the courses prior to each offering. Occasionally, DCIS and/or the OIG LOD will host week-long in-house training courses for field personnel.

41.9.b. **Graduate School USA Courses.** The Graduate School USA offers a wide range of programs and services including continuing education, academic programs, career development, and certificate programs. Field supervisors should coordinate with their regional Graduate School USA offices for additional information (see Attachment C for a list of these offices). The Web site is <http://graduateschool.edu/>.

41.10. Administrative Support Training

41.10.a. Supervisory special agents should research training opportunities for administrative support personnel and provide training based on need, availability, and budget.

41.10.b. Administrative support personnel should be provided administrative training on an annual basis, to include field office and/or HQ-sponsored workshops. The purpose of these workshops is to provide updates on administrative requirements and changing policies, offer the skills/best practices that standardize and enhance efficiency, and deliver the skills necessary for support personnel to be able to perform their functions effectively.

41.10.c. Other administrative training is available as follows and should be offered to the administrative staff whenever possible.

41.10.c.(1). **In-House Courses by OIG DoD** (generally for Washington, D.C., metropolitan area employees only). Schedules and descriptions of these courses are available on the DoD OIG intranet. In addition, the DCIS Training Staff announces course schedules prior to each offering. Occasionally, DCIS and/or the LOD will host an in-house training course for field administrative personnel, which will be announced via e-mail

41.10.c.(2). **Graduate School USA Courses.** The Graduate School USA offers a wide range of regional administrative training courses. The Web site (<http://graduateschool.edu/>) can be searched by subject area for specific information. Courses are exported to various cities across the country, which can be searched on the Web site through: “Courses and Programs” to “Training locations and hotels” to specific search by state and city. (See Attachment C for a list of these offices.)

41.10.c.(3). **FLETC/IG Academy.** FLETC and the IG Academy provide a limited number of non-investigative training courses. Check the Web sites (www.FLETC.gov and <http://www.ignet.gov/igcia/index.htm>) for details on the courses offered.

41.10.c.(4). **Private Vendors.** Private vendors may be used as a training source when governmental training sources are not available or do not fulfill the training requirements. A memorandum request should be forwarded (at least 6 weeks prior to commencement of training) to the Dir-TR with stated justification and concurrence from the cognizant ASAC or SAC. Once approved, an SF-182 must be properly filled out and submitted to the DCIS Training Coordinator. Any registration forms required by the private vendor must also be submitted with the SF-182. Training request procedures are set forth in Attachment B.

41.11. Non-Critical Training

41.11.a. Non-critical training is job-related training that is not essential for performance at the fully successful level. Examples of non-critical training are attendance at community college-level courses, law school, advanced accounting courses, advanced computer training (with exceptions for computer staff), and most law enforcement seminars/conferences.

41.11.b. Requests for non-critical training will be considered on a case-by-case basis and only when the training budget is sufficient. An SF-182 must be completed in DAMIS detailing the exact nature of the training and the benefits to the Agency. (See Attachment B for detailed instructions.)

41.11.c. Requests for critical training will always take priority over non-critical training requests.

41.12. Conferences and Seminars. An Approval/Review Request for Attending Conferences, IG Form 1430.1-4 (May 2013) must be completed fully and adequately by the applicant at least 45 days prior to commencement of any conference/seminar. The package shall be submitted to the DCIS Training Coordinator and will be reviewed by the Dir-TR before being forwarded for approval to DIG INV, OGC, Comptroller’s Office, LOD Conference Coordinator, and final approval by Assistant Inspector General (AIG) for Administration and Management (A&M).

The package must be through all levels of approval before travel to the event may commence and costs incurred. However, travel authorizations may be approved in DTS while awaiting final approval. Again, no travel may occur until package approval is finalized. Emergency approvals should be kept to a minimum.

41.13. Procedures

41.13.a. Each SAC will appoint one field training officer and one alternate to maintain contact with the DCIS Training Staff and coordinate nominations for all announced training events. The field training officer should handle routine training coordination. The name of the field training officer and the alternate should be provided to the DCIS Dir-TR and the DCIS Training Coordinator upon appointment.

41.13.b. All training courses, with the exception of OIG in-house courses (e.g., NEO), and to include free training, ***must*** be submitted on an SF-182 at least 6 weeks before the start of training. Employees are responsible for submitting the SF-182 through their chain-of-command to the DCIS Training Coordinator. The SF-182 is to be submitted correctly and completely (see Attachment B for detailed instructions). Depending on the particular field office practice, the field training officer will either prepare or help prepare all registration forms and SF-182s and ensure these forms are forwarded to the DCIS Training Coordinator. However, it is the responsibility of the employee to ensure the DCIS Training Coordinator has received the completed forms. The DCIS Training Coordinator or a staff member will notify the requestor via e-mail when training has been approved and funded. Failure to comply with this requirement could result in the employee being held responsible for any training costs and any related travel expenses incurred without prior approval.

41.13.c. Trainees will receive specific instructions by e-mail from the DCIS Training Coordinator or FLETC/IGCIA/DCITA scheduler approximately 10 working days prior to training. Special agents will also be directed to read appropriate sections of the “FLETC STUDENT TRAVEL AND INFORMATION GUIDE” for FLETC courses, which are provided to each office and can be found at the FLETC Web site (www.fletc.gov). Special agents will also be provided specific instructions by e-mail from the IG Academy and DCITA for attendance at their respective courses.

41.13.d. Upon completion of all training, ***it is the responsibility of the trainee to provide a copy of their training certificate or proof of completion to their field training officer.*** The field training officer is responsible for uploading the certificate into DAMIS to “complete” the trainee’s DAMIS training record.

41.13.e. Some training events (primarily management training) require specialized nomination forms. The announcements for nominations for such training will contain all necessary procedural information.

41.13.f. Employees are cautioned about scheduling personal travel around official training travel, particularly when an employee has purchased a non-refundable airline ticket in conjunction with official travel. It is possible that a course could be cancelled at the last minute.

41.14. Travel Procedures

41.14.a. **Asset Forfeiture Continuing Education Seminar.** Travel arrangements are processed locally. Travel costs are charged to the asset forfeiture line of accounting.

41.14.b. **Residential Training** (e.g., FLETC, OPM Management Development Seminars, Federal Executive Institute). Directions for preparing orders in the Defense Travel System (DTS) will be furnished to the traveler or can be found in the Admin Tool Box at https://intra.dodig.mil/inv/Admin/admintb_new.htm#TRAVEL. Choosing the correct accounting code and routing path is very important. Typically, the trainee's office training accounting code (e.g., 20FL TR), with the current FY, should be used for training travel unless specified in reporting instructions. Likewise, the travel authorization should be routed through "Training" (dropdown box after digital signature verification) to be processed/funded timely and accurately.

41.14.c. **FLETC.** When preparing a travel authorization for FLETC as a student, there will be no hotel expenses (\$0) and per diem per day is \$5, to include weekends, while in training status. Regular per diem can be claimed for official travel days (usually at 75 percent). Laundry expenses can be claimed during courses that exceed 5 training days; however, a maximum of \$15 will be authorized. Washing facilities are abundantly available and free of charge on FLETC. For WiFi services onboard FLETC, students *must* seek approval from Dir-TR to be reimbursed for STANDARD broadband wireless service in the dorm *prior* to claiming the expense on their travel voucher (**No** exceptions). Otherwise, students may be held personally responsible for the costs incurred. Approval for this expense will be rare. Agents must first use alternate means for Internet connectivity before seeking approval for reimbursement for wireless service. Free LAN connectivity is available in the DCIS Training Academy, Bldg. 66; Internet connectivity is available at the coffee shop located in Bldg. 262. Other training travel policy can be found at Attachment D.

41.14.d. **All Other Training.** Travel arrangements are processed locally. Travel costs (when approved on an SF-182) are charged to the field office training line of accounting (e.g., 20FL TR). In instances where the field office has agreed to fund the travel vice the Training Academy, travel costs are charged to *the field office operational line of accounting*. For assistance, contact the cognizant field training officer or the DCIS Training Coordinator.

41.14.e. **Quarterly Training.** Quarterly control tactics, physical readiness, and firearms training/qualifications are charged to the field office line of accounting if travel expenses are incurred via a travel authorization (TA).

41.14.f. **Cancelled Training.** In the event scheduled training is cancelled, the traveler is responsible for cancelling all reservations in DTS, to include hotel and airline reservations.

ATTACHMENTS

<u>Attachment</u>	<u>Title</u>
A.	Individual Development Plan Information and Instructions
B.	Training Request Procedures
C.	Graduate School USA Regional Training Centers
D.	Training Travel Policy

ATTACHMENT A

INDIVIDUAL DEVELOPMENT PLAN INFORMATION AND INSTRUCTIONS

The official Individual Development Plan (IDP) form is located in the Defense Audit Management Information System (DAMIS). DAMIS is located at <https://damis.dodig.mil/dodig/index.asp> or can be accessed from the DoD OIG intranet Home page under the HR Tools tab in the top banner or from the intranet at <https://damis.dodig.mil/dodig>. Once in DAMIS, the IDP form is located under the “Training” tab. Instructions on completing this form are provided below.

GETTING STARTED

Think about: What do I enjoy doing? What do I do well? What training do I need to perform better? What am I required to do? Where am I going in my job? Where do I see myself in 5 years? In 10 years? What training do I need to get there? What assignments/training do I need to help me reach my goals?

PREPARING THE INDIVIDUAL DEVELOPMENT PLAN

Goal Setting

The short-range goal(s) should be specific and can include anything from obtaining a certain job to mastering a particular skill.

The long-range goal(s) can be more general, such as “senior investigator,” “executive secretary,” or “middle management.”

Necessary Knowledge, Skills, and Abilities

Once you set your goal(s), identify what knowledge, skills, and abilities you need to reach them.

The IDP is recommended to be used as an instrument and guide for career development. First line supervisors are encouraged to use this instrument as a platform to hold annual discussions with their direct reports regarding individual career objectives. Supervisors are encouraged to offer guidance and direction in their employees’ development, although it is the responsibility of the individual to manage his/her own development. Employees are encouraged to seek a mentor either on their own or through the DoD OIG Mentoring Program (https://intra.dodig.mil/A_M/TE/mentoring/index.html). The DCIS Training Staff is available for guidance and recommendations for training courses, as well.

Projected Training

Identify the type of training or developmental activities that will help you gain the knowledge, skills, and abilities you listed. It is not necessary to list only specific courses, nor must the

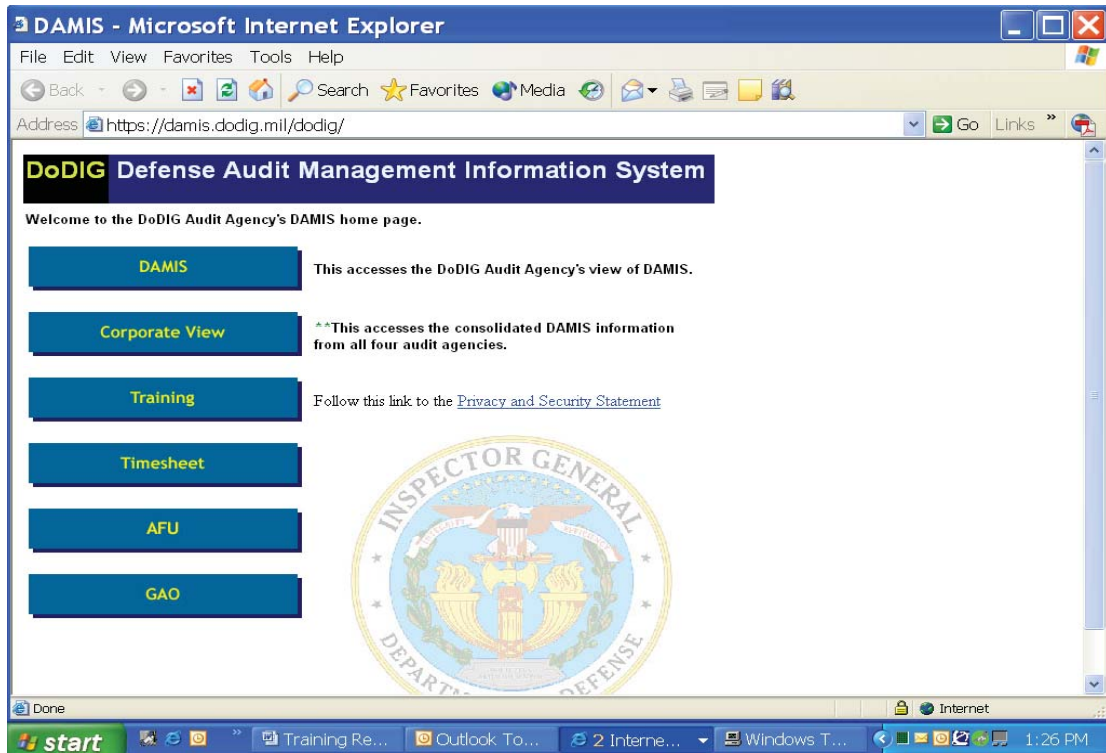
activity be limited to classroom training. Consider on-the-job training, reading, special assignments, distance learning, etc.

Tracking Progress

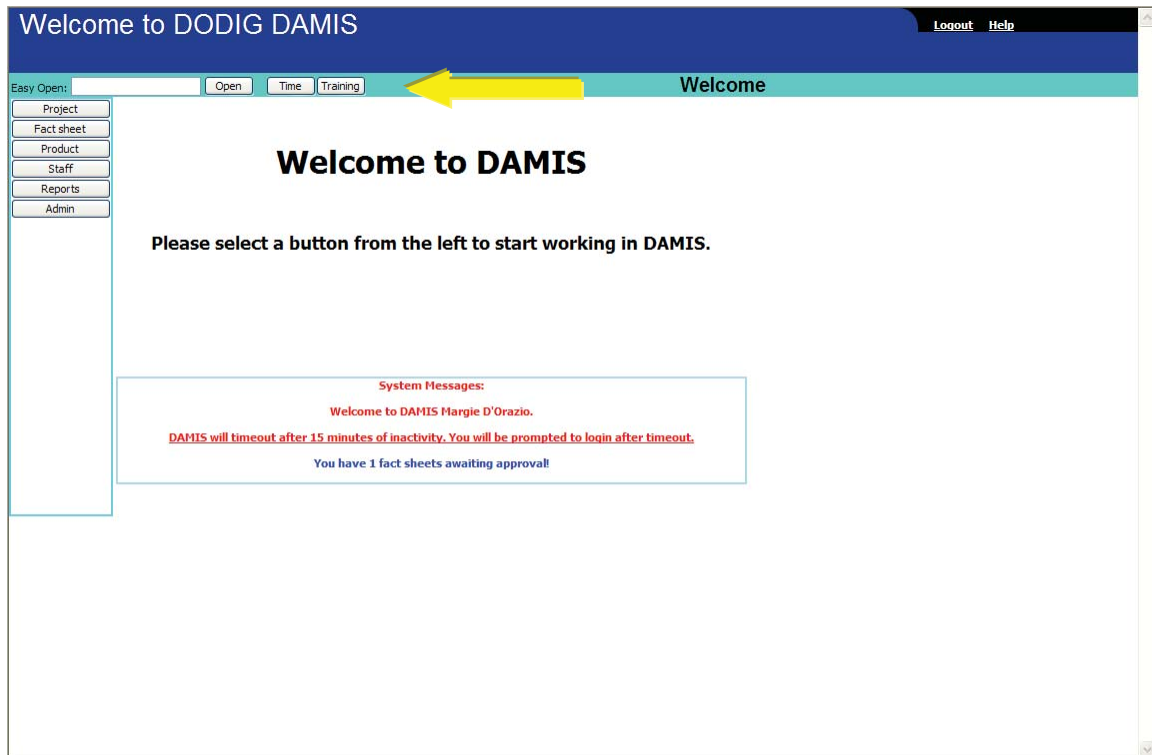
During the year, review your Individual Development Plan every few months and record your training and developmental activities. Discuss your progress with your supervisor. Make changes, if necessary.

MANAGING AN INDIVIDUAL DEVELOPMENT PLAN

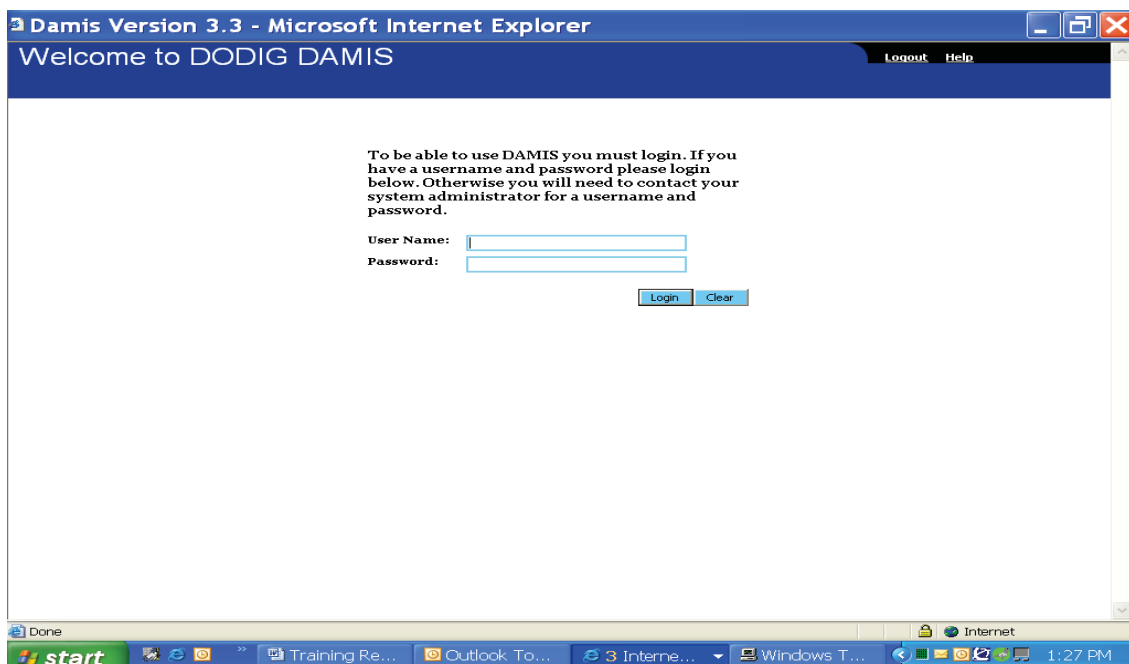
Log on to the DAMIS Web site. Once at the home page, the first time only, either bookmark it or add it to favorites in order to avoid using the IP address every time.



Click on the “Training” button in the Welcome banner.



At the next screen enter your user name and password. Your user name is the same as your DoD login (for example, lmoss). The first time you use the system, your password will be: RESETPASSWORD (Please note that the password is case sensitive.)



If this is the first time you are logging in, the system should tell you that your password has expired and ask you to input a new one. Press “OK.”

<https://damis.dodig.mil/damisdodig/damisLogin.jsp?GOTO=TRAINING> - Microsoft I...



Follow the directions to enter your new password. The system will then require you to log back in with your new password. Please note that the passwords are case sensitive and must be between 9 and 20 characters and must contain at least 2 punctuation symbols (with the exception of &, “(“ or ””) (parentheses)), 2 uppercase letters, 2 lowercase letters, and 2 numbers.

The screenshot shows a web browser window with the address bar displaying `https://damis.dodig.mil/damisdodig/damisLogin.jsp?GOTO=TRAINING`. The page has a blue header bar with a "Change" button. The main content area is white and contains the following text and form elements:

This screen will allow you to change your password.
Passwords must be between 8 and 20 characters
and must contain at least one punctuation symbol with the
exception of '&', '(' or ')'.
Enter your current password below:

Enter your new password:

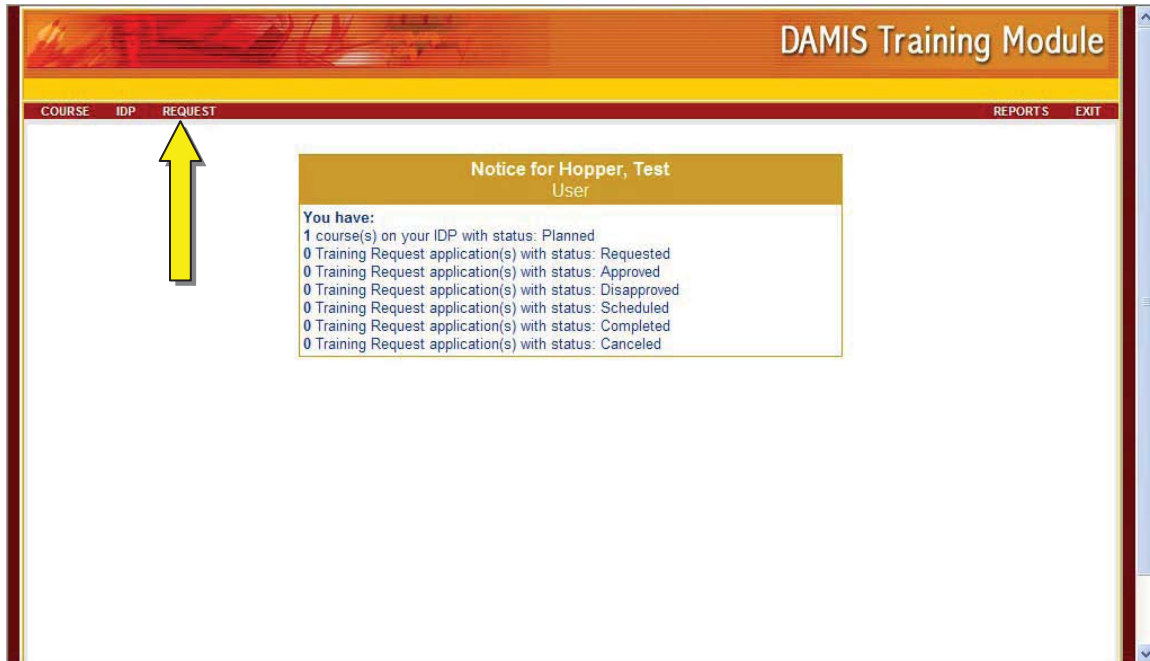
Please type in your new Password
again to confirm:

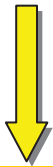
Click the Change button to change your password.

The browser's status bar at the bottom shows "Done" and "Internet". The Windows taskbar at the very bottom includes the Start button, a search bar, and several open applications: Training Re..., Outlook To..., 3 Internet..., and Windows T... The system clock shows 1:31 PM.

Training Module Main Menu Window

At the top of the page there are various tabs. Click on “Request.”





Managing IDP Personal Data

COURSE IDP REQUEST REPORTS EXIT

IDP Personal Data

Included Person: ☒ ACTIVE ☐ ALL Select Person: --Select--

Name	Hopper, Test
Status	ACTIVE
SSN	311121212
Series/Grade	343 / YA02
Position Title	Audit Operations Analyst
Organization	AUD-FO
Duty Station	Arlington, VA
Email Address	margie.dorazio@dodig.mil
Phone Number	
Commercial	703-604-8928
DSN	
FAX Number	
Commercial	703-604-8932
DSN	
Supervisor	--None--
Short-Term (1 year) Objectives	
Long-Term (2-3 year) Objectives	

SUBMIT

Enter/Verify PERSONAL DATA:

Place your mouse over the **IDP** menu bar option.

Select from the list: **Personal Data** - Verify the information (in green fields) that has been entered. If any information is incorrect, send an e-mail to: auditnet@dodig.mil with the correct information to be changed.

Update other fields:

Position Title: Select from the drop-down menu:

E-mail address and Phone Numbers (Commercial, DSN and FAX) (Type)

Select Supervisor name from the drop-down list.

Click **SUBMIT**.

Managing IDP Course Information

This option allows you to view the course(s) listed in your IDP and to add courses to your IDP. Do NOT enter mandatory courses (Ethics, CTIP, Information Assurance, Foreign Travel, etc.) into the IDP. For a complete list, go to A&M, Training Support, and click on Mandatory. The OIG DAMIS team will enter these courses.

1. Place your mouse over the **IDP** menu bar option. Click on **COURSE**. The **IDP Course** window will appear.

Menu
bar

The screenshot shows the 'IDP Course' window. At the top is a menu bar with 'COURSE', 'IDP', 'REQUEST', 'REPORTS', and 'EXIT'. The 'IDP Course' section on the left includes an 'Add a New Course' button and a form with fields for Name (Hopper, Test), Status (ACTIVE), Grade/Series (YA02 / 343), Duty Station (Arlington, VA), and Organization (AUD-FO). To the right, there are filters for 'Included Person' (ACTIVE/ALL), 'Select Person' (dropdown), 'Request Fiscal Year' (list: All, 2012, 2011, 2010), and 'Request Status' (list: All, Planned, Requested, Approved). A 'GO!' button is below the filters. Below the filters, it says 'IDP Courses For Fiscal Year: 2008 Status: ALL'. At the bottom is a table with columns: PRIORITY, COURSE NUMBER, COURSE TITLE, COURSE LOCATION, SD#, COURSE HOURS, TUITION COSTS, OTHER COSTS, TOTAL COSTS, FISCAL YEAR, STATUS, TRAINING REQUEST, 1556 Survey, VIEW CERT., and a 'Delete' link. The table contains one row for course 0118 and a 'TOTALS' row.

	PRIORITY	COURSE NUMBER	COURSE TITLE	COURSE LOCATION	SD#	COURSE HOURS	TUITION COSTS	OTHER COSTS	TOTAL COSTS	FISCAL YEAR	STATUS	TRAINING REQUEST	1556 Survey	VIEW CERT.	
	1	0118	ACQ 201A - Intermediate Systems Acquisition, Part A			37	\$0.00	\$0.00	\$0.00	2008	Planned	view			Delete
TOTALS						37									

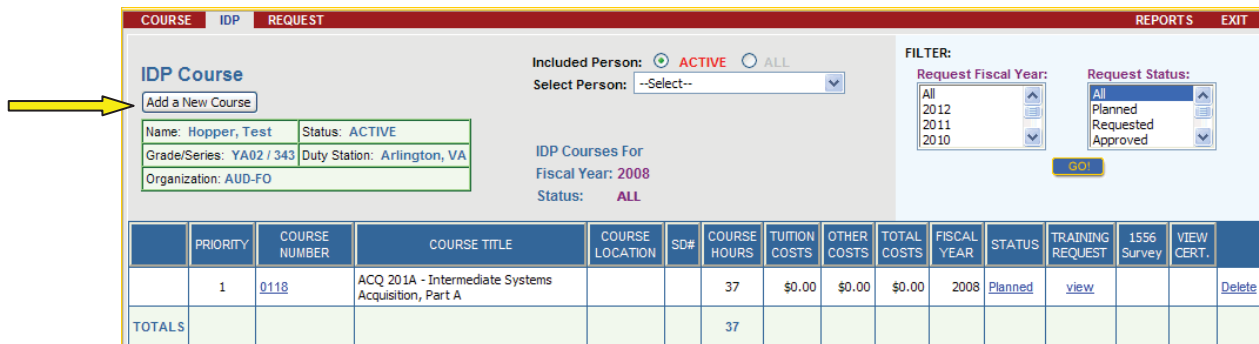
IDP Course Window

The **IDP Course** window defaults to your IDP course information for the current fiscal year. Your employee information is found in the upper left-hand corner of the window, as well as a list of all the courses in your IDP matching the chosen criteria filters.

2. To view course information for other Fiscal Years, select the Fiscal Year(s) and status for which you wish to view requests in the **Request Fiscal Year** and **Request Status** list boxes and click **GO!**. The IDP course listing matching only those criteria will appear.

Adding and Editing New Planned Courses

Follow the steps below to **add new** courses to the IDP.



The screenshot shows the 'IDP Course' main window. At the top, there are tabs for 'COURSE', 'IDP', and 'REQUEST'. A yellow arrow points to the 'Add a New Course' button. The window displays course details for 'Hopper, Test' with status 'ACTIVE'. It also shows filters for 'Request Fiscal Year' and 'Request Status'. Below the details, there is a table of planned courses.

	PRIORITY	COURSE NUMBER	COURSE TITLE	COURSE LOCATION	SD#	COURSE HOURS	TUMON COSTS	OTHER COSTS	TOTAL COSTS	FISCAL YEAR	STATUS	TRAINING REQUEST	1556 Survey	VIEW CERT.
	1	0118	ACQ 201A - Intermediate Systems Acquisition, Part A			37	\$0.00	\$0.00	\$0.00	2008	Planned	view		Delete
TOTALS						37								

1. Click *Add a New Course* button on the *IDP Course* main window. The *Add a Course* window will appear.

Add a New Course to IDP Window

The screenshot shows the 'Add a Course' form within the DAMIS Training Module. The form is titled 'Add a Course' and is located within a window that has tabs for 'COURSE', 'IDP', and 'REQUEST'. The 'COURSE' tab is selected. The form contains the following fields:

- Course Number: A drop-down menu with the text 'Select Course --' and a small 'v' icon.
- Order by: Radio buttons for 'Course #' and 'Title', with 'Title' selected.
- Course Title: A text input field.
- Vendor: A text input field.
- Vendor Address: A text input field.
- Vendor Phone: A text input field.
- Vendor Email: A text input field.
- Course Hours: A text input field.
- Audit-Government Related Hours: A text input field.
- CPE Hours: A text input field.
- Non-CPE Hours: A text input field.
- Fiscal Year: A drop-down menu showing '2008'.
- Priority: A drop-down menu showing '1'.
- IDP Year: A drop-down menu showing '1'.
- Tuition Cost: A text input field.
- Book, Material/Other Cost: A text input field.
- Travel Cost: A text input field.
- Per Diem/Other Cost: A text input field.
- Prefix (Army Only): A text input field.
- MACOM (Army Only): A text input field.
- Objective Accreditation (Army Only): A drop-down menu.
- Course Location: A text input field.
- Comment/Remarks/Objectives: A large text area.

At the bottom of the form are two buttons: 'SUBMIT' and 'CANCEL'. Below the form, there is a link '[view privacy act/notice]' and a copyright notice 'COPYRIGHT 2000-2007 Department of Defense'.

2. Click on the course you want to take from the **Select Course Number** drop-down menu (see window on page 9). The window will refresh and the course title and related course data will automatically populate on the “**Add a Course**” screen. If the course is **not** in the **Select Course Number** menu, then select **TBD** from the drop-down menu. When the screen refreshes, delete “TBD” as the title and enter the real course title and related data fields.
3. If the Vendor information does not automatically populate, complete the Vendor name, Vendor Address, Vendor Phone, and e-mail address (if known).
4. If the **Course Hours**, **Audit-Government Related Hours**, **CPE Hours**, **Tuition Cost** fields do not automatically populate, complete the fields as best you can. Tuition cost must be entered, even if \$0.
5. Select the **Fiscal Year**, **Priority**, and **IDP Year** in which the course will be taken. The **Fiscal Year** and **IDP Year** must be changed to the applicable year the course is to be taken.

6. If the **Comment/Remarks/Objectives** window does not populate, enter your objective for taking the course.

7. Click **SUBMIT**. You will return to the **IDP/ Course** main window and the course is added to the IDP. Repeat process until all desired courses are posted to your IDP.

► Even though this course has now been added to the IDP, it may not show up in the listing on the **IDP Course Main** window. If the Fiscal Year field and Requested Status entries match the Requested Fiscal Year and Requested Status filter criterion that was previously selected, then it will appear upon clicking “Go” and returning to the **IDP Course Main** window.

The screenshot shows the 'IDP Course' window with tabs for 'COURSE', 'IDP', and 'REQUEST'. The 'IDP' tab is active. On the left, there's a form for adding a new course with fields for Name, Status, Grade/Series, Duty Station, and Organization. The 'Name' field contains 'Hopper, Test' and 'Status' is 'ACTIVE'. Below this, it says 'IDP Courses For Fiscal Year: 2008 Status: ALL'. On the right, there's a 'FILTER' section with 'Request Fiscal Year' (All, 2012, 2011, 2010) and 'Request Status' (All, Planned, Requested, Approved). A 'GO!' button is below the filters. At the bottom, there's a table with columns: PRIORITY, COURSE NUMBER, COURSE TITLE, COURSE LOCATION, SD#, COURSE HOURS, TUITION COSTS, OTHER COSTS, TOTAL COSTS, FISCAL YEAR, STATUS, TRAINING REQUEST, 1556 Survey, VIEW CERT., and a 'Delete' link. The table has one row for 'ACQ 201A - Intermediate Systems Acquisition, Part A' with priority 1, course number 0118, 37 hours, and a status of 'Planned'. A 'TOTALS' row at the bottom shows 37 hours.

	PRIORITY	COURSE NUMBER	COURSE TITLE	COURSE LOCATION	SD#	COURSE HOURS	TUITION COSTS	OTHER COSTS	TOTAL COSTS	FISCAL YEAR	STATUS	TRAINING REQUEST	1556 Survey	VIEW CERT.	
	1	0118	ACQ 201A - Intermediate Systems Acquisition, Part A			37	\$0.00	\$0.00	\$0.00	2008	Planned	view			Delete
TOTALS						37									

Other Options for Adding and Editing PLANNED Courses

Editing Course Information

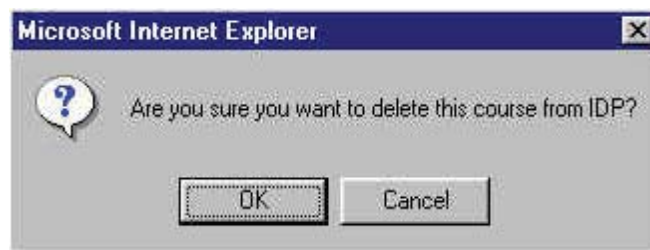
To edit information for a PLANNED course

1. Click on the course number in the **Course Number** column on the **IDP Course** main window (see window on next page). You will proceed to the **Modify a Course** window.
2. Edit the appropriate fields.
3. Click **SUBMIT**. Your changes have been saved and you will return to the **IDP Course** main window.
4. To change a PLANNED course to another FY, go to the Fiscal Year dropdown list and select applicable year and click submit.

Deleting a Course

Any course with a status of PLANNED in the IDP that has not been “Baselined (B)” or approved by the supervisor can be deleted by the employee.

On the **IDP Course** main window, click [Delete](#) in the row of the course you wish to delete. The following message will appear:



Click OK. The course will be removed from the course listing for this IDP.

NOTE: If the status of the course in the IDP is showing “Requested,” only the employee’s supervisor or the cognizant field training officer can delete the course.

ATTACHMENT B

TRAINING REQUEST PROCEDURES

All training, to include no-cost training, must be approved in advance (all electronic signatures obtained – especially if tuition **OR** travel costs are required) before registration with a vendor. All training shall be requested on an electronic Standard Form (SF) 182 through the Defense Audit Management Information System (DAMIS). The field training officer is responsible for ensuring the SF-182 is complete, accurate, and forwarded to the HQ Training Coordinator with a memo of concurrence from the first-line supervisor.

All training requests (whether costs are associated with them or not) should be entered into DAMIS in order to update the student's training history. Information should be put into DAMIS a minimum of 6 weeks prior to the start of the course to ensure registration for the course. If the vendor requires a completed registration form for the class, complete the registration form up to the "payment" section. Forward the form to the HQ Training Coordinator at Headquarters via e-mail for processing. DCIS personnel shall not pre-register or enroll in any class unless it is a "No Cost" course taken locally (no travel cost). The HQ Training Coordinator is responsible for registration/enrollment for **all** courses requiring any funding. The SF-182 request and registration form must be forwarded to the HQ Training Coordinator no less than 6 weeks in advance for processing. If the vendor does not accept payment by Government credit card, the registration package must be submitted to the HQ Training Coordinator at least 8 weeks in advance.

REQUIRED SIGNATURES

Field Offices: The Special Agent in Charge (SAC) or Assistant Special Agent in Charge (ASAC) or designee is authorized to electronically sign in SECTION D, block 1, which is notification of their approval. The FO SAC will notify the DCIS Training Coordinator in writing of his/her designee. Once the SF-182 has been properly completed in the training system, the supervisor must e-mail the DCIS Training Coordinator that a training request awaits approval. If approved, the DCIS Training Coordinator will complete the registration process for the course.

INSTRUCTIONS ON CREATING AN SF-182 IN DAMIS

1. If you are taking **a course that is in your IDP**, create the SF-182 from your IDP. While in the *IDP Course* main window, access Form SF-182 for any course with a status of **Planned** by clicking on **Planned** under the **Status** heading. It is recommended that you complete the SF 182 in the FY that the course will be taken.

COURSE IDP REQUEST REPORTS EXIT

IDP Course

Add a New Course

Name: Hopper, Test Status: ACTIVE

Grade/Series: YA02 / 343 Duty Station: Arlington, VA

Organization: AUD-FO

Included Person: ☒ ACTIVE ☐ ALL

Select Person: --Select--

IDP Courses For
Fiscal Year: 2008
Status: ALL

FILTER:

Request Fiscal Year: All 2012 2011 2010

Request Status: All Planned Requested Approved

GO!

	PRIORITY	COURSE NUMBER	COURSE TITLE	COURSE LOCATION	SD#	COURSE HOURS	TUITION COSTS	OTHER COSTS	TOTAL COSTS	FISCAL YEAR	STATUS	TRAINING REQUEST	1556 Survey	VIEW CERT.
	1	0118	ACQ 201A - Intermediate Systems Acquisition, Part A			37	\$0.00	\$0.00	\$0.00	2008	Planned	view		Delete
TOTALS						37								

The SF 182 will open at the Top Section window. (Skip to 41-B-6, Top Section window and continue.)

2. If you are taking a course that is **NOT** in your IDP, create the SF-182 by
 - a. clicking on **REQUEST** from the menu bar on the *Training Module Main Menu* window.
 - b. Click on the **Select a Course dropdown box**. This box lists all the courses that are currently input in the DAMIS library, but not necessarily all courses that you would want to take. If you know the name of a course DoD IG personnel routinely take, type the first letter of the course title. The cursor will drop to the first course title beginning with that letter. Scroll down and click on the appropriate title. Click on **Add a New Request**.
 - c. If the course is not listed in the library, select **TBD** from the dropdown list and click on **Add a New Request**.

DAMIS Training Module

COURSE IDP REQUEST REPORTS EXIT

Hopper, Test

Fiscal Year: All Request Status: ☐ Requested ☐ Planned

Add a New Request Select a Course

Nothing found to display.

Easy Open: GO!

Request Fiscal Year: All 2012 2011 2010

GO!

Menu bar

d. The SF 182 will open directly into **SECTION B**. This section must be completed and saved before you can proceed. (Go to page 41-B-8 for instructions on completing Section B).

e. Click on “**Save & Go Next.**” *

***NOTE:** If no input/changes are needed, the buttons underneath the opened section will **NOT** highlight. To proceed to the next section, click on the applicable tab (Section A, B, C, etc.). If input/changes are made, the buttons underneath the section will highlight. To save input, click “Save & Go Next.”

► The first time the SF 182 is accessed for a request and changes are saved, the status of the request changes from **Planned** to **Requested**. Once the status is changed to Requested, access the SF 182 by:

- clicking on **Request** in the main menu bar.
- Then check **Requested** and your requested courses will appear on the screen.
- To make changes, click on **edit** located in the right hand column.

DAMIS Training Module

COURSE IDP REQUEST

Hopper, Test
Request for: [Hopper, Test]

Included Person: Hopper, Test
Request Status: ☒ Requested ☐ Planned

Request Fiscal Year: All
Request Responsible Offices: All, A0002A - Office of the Auditor General, D000AB - AB Division, D000AD - AD Division

REQUEST COURSE	REQUEST DATE	REQUEST FOR	REQUEST BY	LAST MOD DATE	TRAINING PERIOD	FUNDING SOURCE	TRAINING REQUEST
ACQ 101 - Fundamentals of Systems Acquisition Management	10/25/2007	Hopper, Test	CPSP Division	10/25/2007 07:10:21 AM	10/25/2007--10/25/2007		view edit delete email supervisor
S+HR Refresher Training for Workers at Hazardous Waste Clean-up Sites (HAZWOPER)	10/17/2007	Hopper, Test	CPSP Division	10/30/2007 05:10:03 AM	10/19/2007--10/18/2007		view edit delete email supervisor

d. The SF 182 will open directly into the **TOP SECTION** window.

TOP SECTION Window

DAMIS Training Module

COURSE IDP REQUEST REPORTS EXIT

View Form SF182

[SELECTING TRAINEE] [TOP SECTION] [SECTION A] [SECTION B] [SECTION C] [SECTION D] [SECTION E] [SECTION F] [COURSE DATA]

Top Section

A. Agency, code agency sub-element, and submitting office number

B. Request Status --Select--

C. Directorate Sponsoring Event: --Select--

D. Type of Transaction --Select--

E. Statement Date (MM/DD/YYYY):

Cancel Save & Go Back Save this Section Save & Go Next

At this screen, fill in blocks “B - D” using the choices in the dropdown boxes.

- a. Block B should be “Initial,” Block “C” should be “DIG-INV,” and Block “D” should be “Other” if FLETC, DCITA, IGCIA or other Govt training; “Check” or “Credit” if an outside vendor (contact the DCIS Training Coordinator if in question).
- b. Click on “Save & Go Next,” which will advance to **SECTION A**.

SF 182: Section A – Trainee Information Window Appears

COURSE IDP REQUEST				REPORTS		EXIT	
[SELECTING TRAINEE]	[SECTION A]	[SECTION B]	[SECTION C]	[SECTION D]	[SECTION E]	[SECTION F]	[COURSE DATA]
Section A - TRAINEE INFORMATION							
1. Name: <input type="text" value="Hopper, Test"/>		2. SSN/EHRI: <input type="text"/>		3. Date of Birth (yyyymmdd): <input type="text"/>			
4. Home Address (Number, Street, City, State, ZIP Code) <input type="text"/>		5. Home Telephone: <input type="text"/>		6. Position Level: <input type="text" value="--Select--"/>			
7. Organization Mailing Address (Branch-Division/Office/Bureau/Agency) <input type="text" value="400 Army Navy Drive Arlington VA 22202-4704"/>		8. Office Telephone: <input type="text" value="703-604-8928"/>		9. Work Email Address: <input type="text" value="margie.dorazio@dodig.m"/>			
10. Position Title: <input type="text" value="Audit Operations Analyst"/>		11. Does applicant need special accommodation? <input type="radio"/> Yes <input checked="" type="radio"/> No If yes, please describe: <input type="text"/>					
12. Type of Appointment: <input type="text" value="--Select--"/>		13. Education Level: <input type="text" value="--Select--"/>					
14. Pay Plan: <input type="text" value="YA"/>		15. Series: <input type="text" value="343"/>		16. Grade: <input type="text" value="02"/>		17. Step: <input type="text"/>	
<input type="button" value="Cancel"/> <input type="button" value="Save & Go Back"/> <input type="button" value="Save this Section"/> <input type="button" value="Save & Go Next"/>							

At this screen fill out blocks 7 8, 9, 10, 14, 15, and 16.

Click on “Save & GoNext,” which will advance to **SECTION B**.

SF 182: Section B – Training Course Data Window Appears

ADMIN ARCHIVE COURSE IDP REQUEST SCHEDULE CPE TRAINING BUDGET REPORTS EXIT									
View Form SF182 Decrement Status									
[SELECTING TRAINEE]	[TOP SECTION]	[SECTION A]	[SECTION B]	[SECTION C]	[SECTION D]	[SECTION E]	[SECTION F]	[COURSE DATA]	[APPROVING]
Section B - TRAINING COURSE DATA									
1a. Training Vendor Name and Mailing Address (No., Street, City, State, ZIP Code) Office of Personnel Management					1b. Location of Training Site <input type="text"/> <input checked="" type="checkbox"/> Same as Block 1a				
1c. Vendor Telephone Number <input type="text"/>					1d. Vendor Email Address <input type="text"/>				
2a. Course Title Telework 101 for Employees					2b. Course Number Code <input type="text"/>				
3. Training Start Date (yyyy-mm-dd) 2010-02-02 ...					4. Training End Date (yyyy-mm-dd) 2010-02-03 ...				
5. Training Duty Hours 1.5					6. Training Non-Duty Hours 0				
7. Training Purpose Type 01 - Program/Mission					8. Training Type Code 02 - Developmental Training Area				
9. Training Sub Type Code 20 - Presupervisory Program					10. Training Delivery Type Code 03 - Technology Based				
11. Training Designation Type Code 03 - Continuing Education Unit					12. Training Credit 1				
13. Training Credit Type Code 03 - Continuing Education Unit					14. Training Accreditation Indicator <input type="radio"/> Yes <input type="radio"/> No <input checked="" type="radio"/> N/A				
15. Continued Service Agreement Required Indicator <input type="radio"/> Yes <input checked="" type="radio"/> No					18. Training Objective Provides employees a brief, practical introduction to telework. It teaches employees strategies for teleworking efficiently, staying in communication with the office, and managing his/her				
16. Continued Service Agreement Expiration Date (yyyy-mm-dd) <input type="text"/> ...									
17. Training Source Type Code 02 - Government External									
<input type="button" value="Cancel"/> <input type="button" value="Save & Go Back"/> <input type="button" value="Save this Section"/> <input type="button" value="Save & Go Next"/>									

If the course is in the course library, the course information will populate into the applicable fields. If not, complete: 1a, 1b, 1c, 1d, 2b, and **All Yellow fields are MANDATORY.**

Block 1a: Mailing address of vendor, phone, and fax number. Please note that the fax number of the vendor is essential to aid in properly registering for the class.

Block 1b: Filled out only if the course is not held at the vendor's primary location. For example, vendor's mailing/registration address is in Hoboken, NJ, and the course is actually being held in Sioux Falls, SD. Put Sioux Falls, SD, in this block.

Block 1c and 1d: self-explanatory.

Block 2a: Course title. **NOTE:** If you selected **TBD as your Course Title**, delete **TBD** from Course Title block and **type in the appropriate course title.**

Block 2b: Enter a Course Code provided by institution, unless a course code is not provided, then enter **N/A.**

Block 3&4: Enter Training Start Date and Training End date using calendar.

Block 5: Enter Training Duty Hours (enter the number of hours; ex: 8).

Block 6: Enter “0” hours for Training Non-Duty Hours or if applicable enter appropriate hours.

Block 11: Unless course has CEU or CPU hours provided, then **N/A** should be selected.

Block 13: If **N/A** is selected in Block 11, then select **01- Semester Hours**. If **CEU** is selected in Block 13, then select **03- Continuing Education Unit**.

Block 18: Training Objective – Self-explanatory (Mandatory even though it’s not highlighted).

Click “Save & Go Next.”

If the SF 182 is accessed from **REQUEST** go back and complete the **Top Section** and **Section A**. Access by clicking on the tabs for the section you need. Save each section.

*For instructions on completing the individual fields in the SF-182 go to the OPM Web site <http://www.opm.gov/forms/html/sf.asp> Load Form SF-182. Click on the links in the fields where you need an explanation. **DO NOT complete the OPM form. You must use DAMIS.**

SF 182: Section C – Cost Information Window Appears

ADMIN ARCHIVE COURSE IDP REQUEST SCHEDULE CPE TRAINING BUDGET

View Form SF182 Decrement Status

[SELECTING TRAINEE] [TOP SECTION] [SECTION A] [SECTION B] [SECTION C] [SECTION D] [SECTION E] [SECTION F] [COURSE DATA]

Section C - COSTS AND BILLING INFORMATION

1. Direct Costs a. Tuition and Fees \$60.00 b. Books & Materials \$0.00 c. TOTAL \$60.00 Appropriation/Fund	2. Indirect Costs a. Travel \$0.00 b. Per diem \$0.00 c. TOTAL \$0.00 Appropriation/Fund
3. Total Training Non-Government Contribution Cost \$0.00	6. Billing Instructions -- Choose Billing Instructions --
4. Document/Purchasing Order/Requisition Number 	
5. 8-Digit Station Symbol 	

Cancel Save & Go Back Save this Section Save & Go Next

This screen pertains to costs related to the training.

All Yellow fields are MANDATORY.

If the selected course is already in the DAMIS library, Blocks 1a and 1b will already be populated.

Block 1a: If not already populated, enter the correct cost if known. If the tuition cost is unknown, enter **\$1.00**. If the course is free of charge, enter **\$0**.*

Block 1b: Enter the correct cost if known. If the books and material are free of charge, enter **\$0**.

Block 2a & 2b: If there is no travel cost, enter **\$0**. If travel/per diem is required, enter the best estimated cost for budgeting purposes.

Block 3: Enter the amount not paid for by Government.

***Note:** If there are no costs associated with the course, fill in Block 6, Billing Instructions, indicating **"No Cost Course"**

Click "Save." You are done.

Note: If you receive a message saying that there are mandatory fields to complete, retype the \$ amount in the box (Example: for number 3. type "0" and click "Save.")

Notify your supervisor that you have completed the SF 182 in DAMIS and that it is awaiting review/approval. Once your supervisor has electronically signed it, e-mail the DCIS Training Coordinator that an SF-182 is in DAMIS waiting approval.

Also, if applicable, forward a completed registration form to the DCIS Training Coordinator.

When a training request has been approved, the DCIS Training Coordinator will inform the student via e-mail.

After the course has been completed, submit a course completion certificate to your field training officer or the Administrative Support Assistant (ASA). The course will be moved to CPE Confirmation History. Once your training certificate has been uploaded, the course will show **completed** in the IDP.

*Note: Who the certificate is sent to will be determined by your Field Office location.

Viewing and Printing Form SF-182

You can access the entire SF-182, with all of the information entered through DAMIS in each section from the top of any of the section windows. In addition to viewing the form in its entirety, you may also print a copy of it.

From any SF-182 section windows, click View Form SF-182.

Form SF-182 opens with Adobe Acrobat Professional.

Click File, Print.

ATTACHMENT C

GRADUATE SCHOOL USA REGIONAL TRAINING CENTERS

Catalogs can be obtained by writing or calling the applicable center listed below, or via the Internet @ <http://www.graduateschool.edu/>

Graduate School USA

Toll-Free Customer Service Center Phone Number (888) 744-GRAD

Toll-Free Fax Number (866) FAX-GRAD

Graduate School USA at Honolulu

Pioneer Plaza

900 Fort Street, Suite 1540

Honolulu, HI 96813-3721

(Classes are NOT held at this location. Please see course detail pages on our website for specific location information.)

Phone: (808) 523-1650

Fax: (808) 523-7634

E-mail: honolulu@graduateschool.edu

[Location Details & Directions](#)

Graduate School USA at Washington, D.C.

Capital Gallery Building

600 Maryland Avenue, SW

Washington, DC 20024

Phone: (202) 314-3300

Fax: (866) FAX-GRAD (866-329-4723)

TDD: (888) 744-2717

E-mail:

customersupport@graduateschool.edu

[Location Details & Directions](#)

ATTACHMENT D
TRAINING TRAVEL POLICY

Purpose:

This document ensures that DCIS employee travel is consistent with the policies of the Joint Travel Regulation (JTR) and DCIS Special Agents Manual Chapter 41. It also defines the specific procedures to be followed when the traveler is utilizing Training travel funds.

Guidance:

The DCIS Training Academy must approve all travel that utilizes the Training Line of Accounting (TR LOA) prior to travel authorizations being created within the Defense Travel System (DTS). Training that is requested and approved through the HQ Training Coordinator and/or Director of Training is considered preauthorized and travel entry into DTS may be made without further approval.

Section 1 – Travel Authorization

Pursuant to DoD policy, all DoD employees are required to use an available Defense Travel Management Office (DTMO)-contracted Commercial Travel Office (CTO). The DODIG CTO for all official transportation requirements (airlines and rental cars) is Carlson Travel.

- 1.1 DTS should be the first method for booking simple airfare and car rental. Calling the CTO to make travel arrangements should only occur for urgent/emergency travel, time constrained bookings, per direction, or when DTS cannot be used to make reservations.
- 1.2 Traveler should create/sign authorization in DTS at least 2 weeks prior to departure date. To avoid airline reservations from being cancelled, DTMO policy mandates all travel authorizations utilizing air travel be approved and ticketed at least 72 hours in advance of the scheduled flight departure. The 2-week lead time allows sufficient time for travel authorizations to be reviewed/approved in order to comply with this policy.
- 1.3 Training travel authorizations should include correct **Trip Purpose:** (DO NOT list Site Visit for Conference attendance). **Trip Description:** should identify the Training/Conference/Meeting attending (SARTP-XXX).
- 1.4 Pertinent information regarding travel should be annotated in **Comments to the Approving Official** or **Pre-Audit Remarks**/justifications.

- 1.5 Authorizations with Air as travel mode – “GSA city-pair contracted airfare” should be selected unless one of the five excludable reasons exists. In the event one of the excludable reasons exists, a detailed explanation must be stated within the Pre-audit justifications.
- 1.6 Mode of Travel other than Air must be notated within the authorization.
- 1.7 Transportation Mode other than Air will require a Constructed Travel Worksheet (CTW). (Travel less than 400 miles one-way or 800 miles roundtrip is automatically considered advantageous to the Government, thus, POV is automatically allowed without CTW.)
- 1.8 The CTW only allows for the traveler to list airfare and CTO fees. No other items will be considered for mileage reimbursement. Traveler must attach a copy of airfare estimate with the CTW.
- 1.9 Individuals flying to FLETC, Glynco, GA, for training are required to use the Jacksonville, FL (JAX) or Savannah, GA (SAV) airport. If the Brunswick, GA, (BQK) airport is no more than \$50 higher than the other airport airfares, traveler may fly into BQK. (Note: BQK airport does not usually provide city pair fares and is generally not the most cost effective airport to utilize when traveling to Glynco for training.)

Section 2- Lodging

- 2.1 Pre-Approval is required for lodging rates that are more than allowed per diem.
- 2.2 Lodging and per diem for students while in travel status at FLETC will be \$0, MI&E \$5, respectively.
- 2.3 Lodging for DCIS sponsored seminar/trainings - travelers should reference reporting instructions before making hotel arrangements. Room blocks with reduced rates to the Government may have been made.

Section 3 – Reimbursable Expenses

Travelers are authorized certain necessary travel and transportation-related reimbursable expenses. Some reimbursable expenses are authorized for reimbursement by the JTR Appendix G; other reimbursable expenses require approval.

- 3.1 Standard baggage fees are reimbursable for travelers on official Government travel. One bag will be authorized for 1 week of travel and two bags are authorized for 2 or more weeks of travel. TRAINING WILL NOT REIMBURSE OVERWEIGHT BAGGAGE FEES.

- 3.2 Laundry for travel that is at least 4 consecutive days is a reimbursable expense. Training will reimburse the amount claimed based upon what a “reasonably prudent person” would incur for the TDY.
- 3.3 Laundry/dry cleaning reimbursement as a FLETC student will be reimbursed at a flat rate of \$5 per week plus cost of laundry supplies. FLETC provides free laundry facilities for students to utilize.
- 3.4 Transportation Tips are reimbursable. Reimbursed fees should be listed as Taxi fare/Tips under non-mileage expenses. Transportation Tips shall be reasonable. Receipts shall be included in documentation uploaded under **Substantiating Records**. Transportation Tips include taxi/shuttle tips. Valet, concierge, and similar tips are not reimbursable.
- 3.5 *Pre-Approval* is needed from Director for Training or Program Manager for reimbursement of internet fees incurred during FLETC TDY.

Section 4 – Voucher Submittal

- 4.1 For other allowable reimbursable expenses, traveler should refer to the JTR.
- 4.2 Receipts are required for all expenses \$75 or more only, unless specified (e.g., transportation tips, during a Continuing Resolution). All lodging receipts are required. Credit card statements cannot be utilized as a form of receipt. Lost receipts for claims that are \$75 or more will need a memorandum of the expense and declaration of the loss receipt.
- 4.3 All receipts are to be uploaded under **Substantiating Records**.
- 4.5 Vouchers are to be completed/signed within 5 business days after end of TDY.



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

January 28, 2016

MEMORANDUM FOR ALL DCIS SPECIAL AGENTS

SUBJECT: Interim Policy for Special Agents Manual (SAM) Chapter 41, "Training," regarding Training History Reviews and Required Training

Effective immediately, this interim policy removes the requirement found in SAM Chapter 41, paragraph, 41.2.h. regarding employee training history reviews. The following language is hereby rescinded:

Office of Quality Assurance and Standards (QAS) verification inspections of the HQ directorates and field offices will include a review of the On-the Job training program (OJT) and every employee's training history to determine whether employees are being scheduled for appropriate training opportunities.

Effective immediately, this interim policy updates SAM Chapter 41, paragraph, 41.3.a. to read as follows:

Required Training. Within the first 18 months of appointment, all criminal investigators are required to attend "core" training, including the Criminal Investigator Training Program (CITP) and the DCIS Special Agent Basic Training (SABT) Program at FLETC or other "equivalent" law enforcement training program.

This policy is in effect until it is rescinded or incorporated into the next revision of SAM Chapter 41. Any questions related to this policy should be directed to me at (703) 604-(b)(6), (b)(7)

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

Deputy Assistant Inspector General
for Investigations

CHAPTER 42

INVESTIGATIVE RECORDS MANAGEMENT

<u>Contents</u>	<u>Section</u>
General	42.1.
Purpose	42.2.
Requirements	42.3.
Authority	42.4.
Creating Records	42.5.
Controls	42.6.
Documentation	42.7.
Constructing and Maintaining	
Case/IR Files	42.8.
Planning Disposition	42.9.
Records Disposition	42.10.
Planning Disposition of Consensual and	
Nonconsensual Interception Recordings	42.11.

42.1. General

42.1.a. This chapter describes the procedures for the creation, construction, maintenance, accountability, retirement, and disposition of Defense Criminal Investigative Service (DCIS) investigative case and Information Report (IR) files (case/IR files) and the controls for the disposal of records and recordings of consensual and nonconsensual monitoring interceptions.

42.1.b. Uniform creation and disposition of records provides for timely retrieval of information throughout DCIS and enhances supervisory review procedures.

42.2. Purpose. An active records disposition program is essential to prevent the accumulation of large quantities of closed investigative case files, IRs, and recordings of consensual and nonconsensual monitoring records in limited office space beyond the time needed to conduct official business.

42.3. Requirements. In accordance with Title 44, United States Code (U.S.C.), sections 3101 and 3303, the head of each Agency is required to establish and maintain a records disposition program to ensure efficient, prompt, and orderly reduction in the quantity of records and to provide for the proper maintenance of records deemed appropriate for permanent preservation.

42.4. Authority. The Federal Records Act of 1950 and the Records Disposal Act, as well as the Federal Property Management Regulations, prohibit destruction of any Federal records without authorization by the Archivist of the United States, National Archives and Records Administration (NARA), pursuant to an approved records disposition schedule. Title 18, United

States Code, specifically sections 641 and 2071, impose penalties, including fines and imprisonment, for unauthorized destruction. Destruction or disposal of classified records is governed by Executive Order 10501.

42.5. Creating Records. The Federal Records Act provides that the head of each Federal agency will establish effective controls over the creation, maintenance, and use of records in the conduct of current business.

42.6. Controls. Controls over the creation of records are essential to ensure that important policies, decisions, and operations are adequately recorded; routine paperwork is kept to a minimum; and the accumulation of unnecessary files prevented. Each field office (FO), resident agency (RA), and post of duty (POD) must apply the following standards and techniques for achieving economy and efficiency in creating records in accordance with general criteria set forth in the Inspector General DoD Instruction (IGDINST) 5015.2, "Records Management Program," November 7, 2007; DCIS Special Agents Manual (SAM) chapters; and other instructions.

42.6.a. Eliminate duplicate files. Take positive action to eliminate duplicate files not required for current operating purposes. Use centralized files, where feasible, to control the growth of individual office working files.

42.6.b. Limit number of copies. Limit the number of documents reproduced and distributed to those required on a strict need-to-know basis.

42.7. Documentation

42.7.a. **Adequacy.** Document the activities of an investigation to the extent necessary to:

42.7.a.(1). facilitate making decisions by agents, managers, prosecutors and other Government officials responsible for decisions on remedies and other actions pursued as the result of DCIS investigations;

42.7.a.(2). fulfill the requirements of Federal statutes;

42.7.a.(3). allow proper scrutiny of investigative operations by Congress and other duly authorized Agencies of the Government;

42.7.a.(4). protect the rights of the Government and of persons affected during an investigation; and

42.7.a.(5). provide material for research.

42.7.b. **Types.** Make all essential information a part of the investigative documentation (refer to Chapter 28 of the SAM for further information). Official investigative documentation

includes communication items such as telegrams, facsimiles, field messages, letters, memoranda, electronic mail (e-mail) transmissions to and from DCIS Headquarters (HQ) or other investigative contacts as deemed necessary and may also include the following.

42.7.b.(1). **Oral Transactions.** Significant oral decisions, commitments, and discussions made in person, by telephone, in staff meetings, or in conferences are a matter of record (as deemed appropriate by the case agent or supervisor). Record this information on one of the following forms:

42.7.b.(1).(a). DCIS Form 1;

42.7.b.(1).(b). Optional Form 271, Conversation Record; or

42.7.b.(1).(c). Memorandum to the File.

42.7.b.(2). **Reports.** Information Reports, Reports of Investigation (ROIs), Forms 1, and other reports prepared by or at the request of HQ or field personnel assigned to the Office of the Inspector General, Department of Defense (OIG DoD) for DCIS are investigative documents. There should be no loose documents (e.g., Interview of “John Doe,” Lead Request) not attached to a report. All documents are attached (stapled, paper clipped, etc.) in the order listed in the report. A master set of all such reports will be maintained as a part of the investigative file.

42.7.b.(3). **Drafts.** Rough drafts of Forms 1 are not retained.

42.7.b.(4). **Investigative Notes.** Original notes on interviews/meetings are maintained as part of the investigative file. The courts have ruled that agents have a legal obligation to maintain original notes, and the agent may be required to produce the notes during legal proceedings. The agent may maintain investigative notes separate from the official case file until the case is closed. Upon completion of the investigation, the investigative notes will be immediately placed in the official case file. All notes must be clearly identifiable to an agent, investigation, and investigative activity.

42.7.b.(5). **Recordings of Consensual and Nonconsensual Monitoring Interceptions.** See section 42.11. below.

42.8. Constructing and Maintaining Case/IR Files

42.8.a. A case/IR file is defined as a folder or other file unit (binder, accordion keeper, etc.) identified by a unique identifier (UID) as assigned by the Investigative Data System (IDS) to a particular title given to an investigation or inquiry. This file will contain material relating to the specific action, transaction, event, person, place, project, or other subject. A case/IR file may include one or more subjects that relate to a specific investigation.

42.8.b. The official file for open case/IR files will be maintained at the FO, RA, or POD (when approved by the FO Special Agent in Charge) conducting the investigation. Headquarters will not maintain duplicate file folders. However, the Case Initiation Report (CIR), Case Summary Updates (CSU), ROI/Case Termination, and IRs will be current and on line in the IDS.

42.8.c. The DCIS investigative files will be organized and maintained according to the following.

42.8.c.(1). Use 8-1/2 by 11-inch folders, preferably heavy cardboard.

42.8.c.(2). Separate file folder(s) for each individual investigation or inquiry. In those incidents involving joint investigations between two or more DCIS offices, refer to SAM Chapter 28 for further guidance.

42.8.c.(3). Each investigative case/IR file will depict the UID and title clearly marked on the outside of the folder.

42.8.c.(4). The CIR, with any attachments, will be filed on the left side of the file folder. Place the file in reverse chronological order (oldest document on the bottom).

42.8.c.(5). The DCIS-INV Form 50, (Case) Index Sheet (Attachment A), is filed on the left side of the folder as a cover document. The Case Index Sheet serves as a log for all material within the folder and provides a means to rapidly review the contents of any investigative file. It is recommended the form be used; however, its use is optional.

42.8.c.(6). The Sign-Out Sheet (Attachment B) is filed on the left side of the folder and is used to log/track all persons that review the case/IR(s) file.

42.8.c.(7). The DCIS Form 57, Disclosure Accounting Sheet (Attachment C) is filed on the left side of the folder and is used to log persons from outside DCIS who have a need to review the case/IR(s) file.

42.8.c.(8). The FOIA/Privacy Act Form (Attachment D) is filed on the left side of the folder and is used by Freedom of Information Act and Privacy Act (FOIA/PA) personnel to document FOIA/PA requests and to whom and what information was released on the closed investigative case file. All FOIA/PA requests about DCIS investigations are handled in accordance with SAM Chapter 48.

42.8.c.(9). All Forms 1 or “other materials” that would enhance a chronological review of the case file from inception to completion are filed on the right side of the folder. A few examples of “other materials” that meet this criteria are Case Summary Reports, ROIs, Significant Incident Reports, Polygraph Examination Reports, newspaper articles, signed OAIG-INV Forms 2, [WARNING] Retention Control Sheets, and other types of correspondence. See section 42.11. for information concerning consensual monitoring audiotapes or videotapes.

42.8.c.(10). **NOTE:** Paragraphs 42.8.c.(1). through 42.8.c.(6)., above, are guidelines for how to construct a case file. However, minor variations of the above are permitted within the case files at the FOs, when the following rules are applied:

42.8.c.(10).(a). the variation is the same throughout a given FO;

42.8.c.(10).(b). DCIS HQ, Internal Operations Directorate (IOD) approves the variation. (Follow the same procedures used when asking for variations in the filing of administrative documents.)

42.8.d. Grand jury material will be handled in accordance with SAM Chapter 15, “Grand Jury Proceedings,” and appropriate Federal regulations. However, grand jury material obtained during an investigation will be maintained at the office of origin. DCIS HQ will maintain copies of grand jury material only for the following reasons:

42.8.d.(1). grand jury material obtained while working special operations, undercover, or HQ controlled cases; or

42.8.d.(2). if it is necessary for the grand jury material to be retained/retired with the case file. A letter of disposition from the Assistant U.S. Attorney attached to the grand jury envelope is required.

42.9. Planning Disposition. The ultimate disposition of every case file is its retention by the Washington National Records Center (WNRC), in Suitland, MD, for disposable records or NARA, College Park, MD, for permanent records as deemed appropriate. Closed IRs and investigative case files are held by field components for 2 years, then forwarded to DCIS HQ for transfer to the WNRC. As authorized by IGDINST 5015.2, “Records Management Program,” Series 800 – Investigations, IRs are destroyed 10 years from the date of closure, and the investigative case files are destroyed 25 years after closure unless qualified for permanent retention. However, there are minor exceptions. Offices are required to maintain their case/IR files in a manner that facilitates proper disposition and transfer to DCIS HQ for further transfer to the WNRC. To accomplish this, offices must accomplish the following.

42.9.a. Establish file breaks by segregating active from inactive (open from closed) files and investigative case files from IRs. This action makes disposition easier because the final disposition of records is normally based on the type of file and the closing date of the file. The closing date of the file is derived from the date entered in the “closed date” field in the IDS.

42.9.b. Indicate the closing date (CD) of the file clearly on the front of the folder (example: CD - May 2010; CD - June 2011, etc.).

42.9.c. The Special Agent in Charge, or designee, is responsible for coordinating the removal/purging of duplicate and unnecessary documents in the official file(s) prior to shipment to DCIS HQ. Grand jury materials will be disposed of in accordance with paragraph 42.8.d.

42.9.d. Review disposition practices periodically to ensure approved disposition instructions are properly applied.

42.10. Records Disposition

42.10.a. DCIS HQ will notify field elements and provide each a list of closed case/IR files, based on IDS/UID information, to be submitted to DCIS HQ for retirement to the WNRC. The files are to be boxed and shipped to DCIS HQ via a parcel shipping service with tracking, such as FedEx or a similar service. Each box must be numbered in sequence, for example, 1 of 10, 2 of 10, etc. A list depicting the case control number, case title, FO/RA/POD and the opening and closing date of each case file being retired must be in the first box of the shipment to DCIS HQ. Grand jury material should be submitted independently of the case file to DCIS HQ. The exterior cover of the grand jury material will be annotated that the case file is being shipped separately.

42.10.b. Upon receipt of records at DCIS HQ, IOD personnel will:

42.10.b.(1). verify the number of boxes in the shipment;

42.10.b.(2). open boxes and compare file list with actual folders in box(es);

42.10.b.(3). if the file list and folders do not correspond, IOD personnel will immediately notify the field element to rectify the discrepancy. ALL official case/IR files identified by IDS/UIDs must be accounted for; and

42.10.b.(4). if a file identified by the IDS/UID cannot be accounted for, the field element is required to prepare a memorandum documenting steps taken to locate the missing file(s) along with the steps taken to reconstruct the file(s).

42.10.c. To reconstruct a missing case/IR file, print from IDS/UID a copy of the following:

42.10.c.(1). CIR;

42.10.c.(2). Most recent CSU;

42.10.c.(3). Final ROI/Case Termination Form 1;

42.10.c.(4). Data screens for the UID and all subjects thereof;

42.10.c.(5). For IRs, print only the CIR from the IDS/UID; and

42.10.c.(6). Create a new folder(s) and forward to DCIS HQ.

42.11. Planning Disposition of Consensual and Nonconsensual Interception Recordings

42.11.a. **Records Administration.** To preclude unauthorized access, theft, or use, all recordings and records of consensual recordings obtained through interception activities conducted under the provisions of SAM Chapter 11, “Interception of Wire, Electronic, and Oral Communications,” will be safeguarded. The interests of the Government and the rights of private individuals involved were considered in the development of these procedures. This chapter implements the following procedures for the storage and access requirements of recordings and other records of information obtained through interception activities. It includes provisions for storage and access after the case becomes inactive and the records and recordings are transferred to a centralized facility. The centralized facility resides within the IOD at DCIS HQ.

42.11.b. **Indexing and Marking for Identification Purposes.** The recordings of consensual and nonconsensual monitoring interceptions shall be prepared and maintained to provide for centralized, readily accessible records or indices.

42.11.b.(1). There are several types of recording media: magnetic, optical, and paper. They include, but are not limited to, audiocassettes (micro and standard), videocassettes and reel-to-reel tapes, digital recorders, and micro SD cards that are used in digital recorders, CDs, and DVDs.

42.11.b.(2). These recordings must be marked individually on the recording itself and on the envelope or folder. Use shipping instructions already established for investigative case/IR files.

42.11.c. **Retention and Disposition of Recordings.** The original records and media recordings of oral interceptions are to be maintained for the life of the investigative case file in accordance with DoD Directive 5200.24. and retirement procedures established in coordination with NARA. The recordings are maintained separate from the “paper” files at the WNRC.

42.11.c.(1). Erase and dispose of all copies. Erased magnetic media is reused for copy purposes only. Do not use erased magnetic media for original records.

42.11.c.(2). If the Title III wire interception was conducted in the United States under the provisions of 18 U.S.C. § 2516 (Title III - Wire Intercepts), the records may only be destroyed pursuant to an order of the court involved. If the court orders that the recordings be disposed of as soon as the trial is over, the recordings may be disposed of at the field element. If the court orders that the recordings be retained, forward them to DCIS HQ with a letter stating the disposal instructions. **DO NOT** send Title III - Wire Intercept recordings to IOD without a letter of disposal instructions from the court involved.

42.11.c.(3). Upon formal request from DCIS HQ, forward consensual and non-consensual recordings to IOD. Upon receipt in IOD, they will be arranged by year closed and

UID and retired to the WNRC. On the appropriate disposal date, the recordings are destroyed (burned) to eliminate reusing the tapes or jeopardizing the integrity of the material.

42.11.c.(4). Text transcripts of consensual or nonconsensual monitoring recordings will be retained in the investigative case file and sent to DCIS HQ only when the investigative case file is being retired.

ATTACHMENTS

<u>Attachment</u>	<u>Title</u>
A	DCIS-INV Form 50, Index Sheet
B	Sign-Out Sheet
C	DCIS Form 57, Disclosure Accounting Sheet (Public Law 93-579)
D	FOIA/PRIVACY Form

DCIS-INV FORM 50, INDEX SHEET

FOR OFFICIAL USE ONLY

SIGN-OUT SHEET

Name

[illegible]

ATTACHMENT C

DISCLOSURE ACCOUNTING SHEET

(Privacy Act of 1974, Public Law 93-579)
(DoD Directive 5400.11, "DoD Privacy Act Program")

Subject's full name, Social Security number, date of birth:

Recipient's name, agency, and address:

Purpose of disclosure (ROUTINE USE):

COPY PROVIDED: Yes No

Date of disclosure:

Description of material disclosed (Date of ROI and CCN. If disclosure was not total, identify information disclosed by paragraph number and identification of attachments.):

DCIS FORM 57

42-C-1

August 2011

ATTACHMENT D

FOIA/PRIVACY FORM

FOIA/PRIVACY

This file, or portions thereof, has been requested under the Freedom of Information Act and/or Privacy Act (FOIA/PA).

The FOIA/PA file referenced below sets forth information regarding the documents released.

Request Number _____
Name of Requestor _____
Date of Release _____

Request Number _____
Name of Requestor _____
Date of Release _____

Request Number _____
Name of Requestor _____
Date of Release _____

Request Number _____
Name of Requestor _____
Date of Release _____



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

September 21, 2017
Ref: DODOIG-2017-000193

SENT VIA EMAIL

This is the final response to your Freedom of Information Act (FOIA) request for a copy of the Defense Criminal Investigative Service (DCIS) Special Agents Manual. We received your request on December 31, 2016, and assigned it case number DODIG-2017-000193.

The Defense Criminal Investigative Service conducted a search and found the enclosed documents, which consist of Chapters 46 through 59 of the Special Agents Manual, as responsive to your request. After carefully reviewing the records, I have determined that 236 pages of records are appropriate for release in full, copies of which are enclosed. Additionally, I have determined that 22 pages of records are appropriate for release in part, and that 226 pages of records are exempt from disclosure pursuant to:

- 5 U.S.C. § 552 (b)(2), which relates solely to the internal personnel rules and practices of an agency;
- 5 U.S.C. § 552 (b)(6), which pertains to information, the release of which would constitute a clearly unwarranted invasion of personal privacy;
- 5 U.S.C. § 552 (b)(7)(C), which pertains to records or information compiled for law enforcement purposes, the release of which could reasonably be expected to constitute an unwarranted invasion of personal privacy; and
- 5 U.S.C. § 552 (b)(7)(E), which pertains to records or information compiled for law enforcement purposes, the release of which would disclose techniques and procedures for law enforcement investigations or prosecutions.

In view of the above, you may consider this to be an adverse determination that may be appealed to the Department of Defense, Office of Inspector General, ATTN: FOIA Appellate Authority, Suite 10B24, 4800 Mark Center Drive, Alexandria, VA 22350-1500. Your appeal, if any, must be postmarked within 90 days of the date of this letter and should reference the file number above. I recommend that your appeal and its envelope both bear the notation "Freedom of Information Act Appeal."

September 21, 2017
Ref: DODOIG-2017-000193

You may seek dispute resolution services and assistance with your request from the DoD OIG FOIA Public Liaison Officer at 703-604-9785, or the Office of Government Information Services (OGIS) at 877-684-6448, ogis@nara.gov, or <https://ogis.archives.gov/>. Please note that OGIS mediates disputes between FOIA requesters and Federal agencies as a non-exclusive alternative to litigation. However, OGIS does not have the authority to mediate requests made under the Privacy Act of 1974 (request to access one's own records.)

Please note that this office has now completed the processing of your request and your request is being closed. If you have any questions regarding this matter, please contact Searle Slutzkin at 703-699-7520 or via email at foiarequests@dodig.mil.

Sincerely,

A handwritten signature in black ink, appearing to read "Mark Dorgan", with a long horizontal flourish extending to the right.

Mark Dorgan
Division Chief
FOIA, Privacy and Civil Liberties Office

Enclosure(s):
As stated

CHAPTER 47

PERFORMANCE MANAGEMENT

<u>Contents</u>	<u>Section</u>
Purpose	47.1.
Performance Appraisal Periods	47.2.
Performance Plans	47.3.
Annual Performance Ratings	47.4.
Performance Award Nominations	47.5.

47.1. Purpose. This chapter supplements Inspector General Regulation (IGDR) 1400.430, “Performance Management,” dated January 19, 2010 (available on the intranet). This chapter applies to the Office of the Deputy Inspector General for Investigations (DIG-INV), Defense Criminal Investigative Service (DCIS) employees. It delegates authority to the Headquarters Assistant Inspectors General for Investigations (AIGI) and Special Agents in Charge (SAC) to approve Summary Ratings, Performance Awards, Superior Accomplishment Awards, and Time-Off Awards. The Inspector General is the approving official for Quality Step Increases.

47.2. Performance Appraisal Periods. The annual performance appraisal period for employees assigned to DCIS is October 1 through September 30 of the current fiscal year.

47.2.a. The rating period will begin as the date of the employee’s entrance on duty when an employee is not assigned to DCIS as of October 1.

47.2.b. The rating period will be shortened if a change in position or supervision occurs after July 1. In such cases, the rating of record will assess the employee’s performance from October 1 of the current fiscal year (or the day he/she enters on duty with DCIS) to the day before the change in position or supervision becomes effective. The employee’s subsequent appraisal period will begin on the day the change in position or supervision becomes effective, and will end on September 30 of the following fiscal year (e.g., if an employee is promoted on July 15, 2010, then his/her appraisal period for that year will end on July 14, 2010, and he/she will receive a rating of record assessing his/her performance from October 1, 2009, to July 14, 2010. The appraisal period for the following year will begin on July 15, 2010, and end on September 30, 2011).

47.3. Performance Plans

47.3.a. Employee Performance Plans will be completed by the employee’s first-level supervisor, then reviewed and approved by the employee’s second-level supervisor within 30 days of the beginning of the rating period. NOTE: The employee does not sign the Employee Performance Plan until after it has been reviewed and approved by the second-level supervisor.

47.3.b. The development, review, and approval of Employee Performance Plans for DCIS supervisory personnel will be as follows:

47.3.b.(1). Field Office Personnel

47.3.b.(1).(a). SAC

Directorate (INV-OPS) 47.3.b.(1).(a).i. Supervisor–AIGI, Investigative Operations

47.3.b.(1).(a).ii. Reviewer/Approving Official–DIG-INV

47.3.b.(1).(b). Assistant Special Agents in Charge (ASAC)

47.3.b.(1).(b).i. Supervisor–SAC

47.3.b.(1).(b).ii. Reviewer/Approving Official–AIGI-INV

47.3.b.(1).(c). Resident Agents in Charge (RAC)

47.3.b.(1).(c).i. Supervisor–ASAC

47.3.b.(1).(c).ii. Reviewer/Approving Official–SAC

47.3.b.(2). Headquarters Personnel

47.3.b.(2).(a). SAC, INV-OPS

47.3.b.(2).(a).i. Supervisor–AIGI-INV

47.3.b.(2).(a).ii. Reviewer/Approving Official–DIG-INV

47.3.b.(2).(b). Program Director (PD)

47.3.b.(2).(b).i. Supervisor–SAC, INV-OPS

47.3.b.(2).(b).ii. Reviewer/Approving Official–AIGI, INV

47.3.b.(2).(c). SAC, International Operations Directorate (INTL-OPS)

47.3.b.(2).(c).i. Supervisor–AIGI, INTL-OPS

47.3.b.(2).(c).ii. Reviewer/Approving Official–DIG-INV

47.3.b.(2).(d). Program Director (PD)

47.3.b.(2).(d).i. Supervisor–SAC, INTL-OPS

47.3.b.(2).(d).ii. Reviewer/Approving Official–AIGI, INTL

47.3.b.(2).(e). SAC, Internal Operations Directorate (INT-OPS)

47.3.b.(2).(e).i. Supervisor–AIGI, INT-OPS

47.3.b.(2).(e).ii. Reviewer/Approving Official–DIG-INV

47.3.b.(2).(f). Program Director (PD)

47.3.b.(2).(f).i. Supervisor–SAC, INT-OPS

47.3.b.(2).(f).ii. Reviewer/Approving Official–AIGI, INT-OPS

47.4. Annual Performance Ratings

47.4.a. The employee's first-level supervisor will serve as the rating supervisor, the second-level supervisor as the Reviewer, and the third-level supervisor as the Approving Official on the Employee Performance Rating. The second-level supervisor may serve as both the Reviewer and Approving Official if he/she is a DIG, AIGI, or SAC.

47.4.b. The supervisory chain for Employee Performance Ratings for DCIS field office supervisory employees is the same as for the development, review, and approval of Employee Performance Plans for DCIS field office supervisory personnel as listed above.

47.4.c. Two copies of the completed Employee Performance Rating, two copies of the Employee Performance Plan, and, if applicable, the original and one copy of the Award Nomination form will be submitted to the Human Capital Management Directorate (HCMD), Workforce Relations Division (WRD) through the DIG-INV following the end of the employee's annual rating period. IGDR 1400.430 states that completed ratings are due in the HCMD-WRD not later than 30 calendar days following the end of the rating period. Budget and Personnel, INT-OPS will forward all forms to HCMD-WRD within 30 calendar days following the end of the employee's rating period.

47.5. Performance Award Nominations

47.5.a. The supervisory chain for award nominations for Headquarters employees will include the nominating official, reviewer, and approving official. The reviewer and approving official may be the same individual if he/she is a DIG, AIGI, or SAC.

47.5.b. The supervisory chain for award nominations for DCIS field office supervisory employees is the same as for the development, review, and approval of Employee Performance Plans for DCIS field office supervisory personnel.

CHAPTER 48

ACCOUNTING FOR DISCLOSURE OF INFORMATION FROM DEFENSE CRIMINAL INVESTIGATIVE SERVICE RECORDS

<u>Contents</u>	<u>Section</u>
General	48.1.
Purpose	48.2.
Procedures	48.3.
Applicable Laws, Regulations, and Directives	48.4.
Definitions	48.5.
Freedom of Information Act Requirements	48.6.
Privacy Act Requirements	48.7.
Information Obtained From Financial Institutions	48.8.
Disclosure Accounting	48.9.

48.1. General. The records compiled and maintained by the Defense Criminal Investigative Service (DCIS) must be safeguarded in such a manner that they are released only to those individuals having a legitimate need to see the information.

48.2. Purpose. This chapter revises the established procedures to be followed when accounting for the disclosure of information from DCIS record systems.

48.3. Procedures. The procedures described in this chapter apply to DCIS Headquarters and all DCIS field elements of the Office of the Inspector General of the Department of Defense (OIG DoD).

48.4. Applicable Laws, Regulations, and Directives

48.4.a. Public Law 95-452, “Inspector General Act of 1978,” as amended.

48.4.b. Title 5, United States Code (U.S.C.), section 552, “Freedom of Information Act,” as amended.

48.4.c. Title 5, U.S.C., section 552a, “Privacy Act of 1974,” as amended.

48.4.d. Title 12, U.S.C., section 3401 et seq., Public Law 95-630, “Right to Financial Privacy Act of 1978,” 92 Stat. 3697, November 10, 1978.

48.4.e. Title 32, Code of Federal Regulations (CFR), Part 312, “Office of the Inspector General Privacy Program,” October 17, 1991.

48.4.f. DoD Regulation 5200.1-R, “Information Security Program,” January 1997.

48.4.g. DoD Regulation 5400.7-R, “DoD Freedom of Information Act Program,” Change 1, April 11, 2006.

48.4.h. DoD Regulation 5400-11.R, “Department of Defense Privacy Program,” May 14, 2007.

48.4.i. DoD Directive 5106.01, “Inspector General of the Department of Defense,” Change 1, September 25, 2006.

48.4.j. DoD Directive 5400.07, “DoD Freedom of Information Act (FOIA) Program,” January 2, 2008.

48.4.k. DoD Directive 5400.11, “DoD Privacy Program,” May 8, 2007.

48.4.l. DoD Instruction 5400.15, “Guidance on Obtaining Information From Financial Institutions,” Change 1, July 3, 2007.

48.4.m. USD(I) Directive-Type Memorandum 04-010, “Interim Information Security Guidance,” April 16, 2004.

48.4.n. Inspector General Instruction 4630.1, “Electronic Mail Policy,” May 22, 2007.

48.4.o. Inspector General Instruction 5400.7, “Freedom of Information Act (FOIA) Program,” April, 16, 2010.

48.4.p. Inspector General Instruction 5400.11, “Privacy Act Program,” January 29, 2010.

48.4.q. Inspector General Policy Memorandum 2003-20, “Release of OIG Reports Containing Privacy Act Protected Information,” August 29, 2003.

48.4.r. Inspector General Policy Memorandum 2004-21, “Electronic Mail Transmission of Information Designated as “For Official Use Only,” June 28, 2004.

48.5. Definitions

48.5.a. **Agency.** Any executive department, military department, Government-controlled corporation, independent regulatory agency, or other establishment in the executive branch, except the actual Office of the President. (The Privacy Act does not apply to the legislative or judicial branches.)

48.5.b. **Disclosure.** The transfer of any personal information from a system of records by any means of communication (such as oral, written, electronic, mechanical, or actual review) to any person, private entity, or Government agency, other than the subject of the record, the subject’s designated agent, or the subject’s legal guardian.

48.5.c. **Federal Register.** Established by the United States Congress to inform the public of interim, proposed, and final regulations or rule-making documents having substantial impact on the public. It is published daily and provides a uniform system for the publication of Presidential and Federal agency documents that concern the public and are required to be published by statute.

48.5.d. **Financial Institution.** Any office of a bank, savings bank, credit card issuer, industrial loan company, trust company, savings and loan, building and loan, homestead association (including cooperative banks), credit union, or consumer finance institution that is located in any state or territory of the United States, or in the District of Columbia, Puerto Rico, Guam, American Samoa, or the Virgin Islands.

48.5.e. **Individual.** A citizen of the United States or an alien lawfully admitted for permanent residence.

48.5.f. **Law Enforcement Activity.** Any activity engaged in the enforcement of criminal laws, including efforts to prevent, control, or reduce crime; or to apprehend criminals; and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities.

48.5.g. **Maintain.** Includes maintain, collect, use, or disseminate.

48.5.h. **Records**

48.5.h.(1). Under the Privacy Act (PA), a “record” is any item, collection, or grouping of information about an individual that is maintained by an Agency that contains an individual’s name, Social Security number, or other identifying particular.

48.5.h.(2). Under the Freedom of Information Act (FOIA), an “Agency record” is the product of data compilation, such as books, papers, maps, and photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an Agency of the United States Government under Federal law in connection with the transaction of public business and in the possession and control of the OIG DoD at the time a FOIA request is made.

48.5.i. **Routine Use.** The disclosure of a record outside DoD for a use that is compatible with the purpose for which the information was collected and maintained by DoD. The routine use must be included in the published system notice for the system of records involved.

48.5.j. **System of Records.** A group of any records under the control of any Agency from which information is retrieved by the name of the individual or by some identifying particular assigned to the individual. System notices for all PA systems of records must be published in the Federal Register.

48.6. Freedom of Information Act Requirements

48.6.a. **References.** Paragraphs 48.4.b., g., and o.

48.6.b. **Policy.** The public has a right to information concerning the activities of its Government. It is OIG DoD policy to conduct its activities in an open manner and to provide the public with the maximum amount of accurate and timely information concerning its activities, consistent always with the legitimate public and private interests of the American people.

48.6.c. **Procedures.** All FOIA requests received by a DCIS field element, and a copy of all responsive information, must be forwarded promptly to the Office of Communications and Congressional Liaison, Freedom of Information Act and Privacy Act (FOIA/PA) Office. The DCIS field element will advise the requester in writing that his/her request was forwarded to the FOIA/PA Office for further action (see **Attachments A and B**). Requests received by offices located at Headquarters will be hand-carried to the FOIA/PA Office.

48.6.c.(1). The FOIA/PA Office will task the Internal Operations Directorate (IOD) via e-mail on all requests. IOD will locate the DCIS case records and determine whether the appropriate documents are available.

48.6.c.(2). This task will be forwarded via e-mail to the DCIS field element having operational control of the investigation, with an information copy to the appropriate field office, when applicable. The field element maintaining the case file will have 10 days to respond to IOD via e-mail with the following information:

48.6.c.(2).(a). verification as to whether the case is open or closed;

48.6.c.(2).(b). a statement concurring or nonconcurring with the proposed release of the requested documents on both open and closed cases, since either may jeopardize an investigation;

48.6.c.(2).(c). in the case of a nonconcurrence of release, a statement justifying the recommendation for denial of the request, with appropriate reasons;

48.6.c.(2).(d). a brief summary of the documents that have been located and status of forwarding them to IOD;

48.6.c.(2).(e). a point of contact, including telephone number, should be listed if further coordination is required.

48.6.c.(3). The field element will send a copy of the pertinent document(s) to IOD. On receipt of the above information and/or documents from the field element, IOD will provide a consolidated response to the FOIA/PA Office. (NOTE: Pertinent documents should NOT be sent via express/overnight mail unless requested; regular first-class mail is sufficient.)

48.6.c.(4). When the FOIA/PA Office request involves multiple cases or complex issues, the action will be coordinated with the appropriate Investigative Operations Directorate program personnel for an investigative review of the records.

48.6.c.(5). On receipt of the consolidated response from IOD, the FOIA/PA Office will evaluate all pertinent documents and prepare a response to the requester. Copies of the e-mail messages will be retained in the work folder to support the basis for any denials. The Chief, FOIA/PA Office, may coordinate the final response with the appropriate field element via telephone or e-mail to resolve issues.

48.6.c.(6). On all closed cases where the case file has been submitted to headquarters, IOD will locate and search the file for the pertinent document(s). The appropriate field element(s) will be notified via e-mail message of the request and the pending release. The field element will have 10 days to concur or nonconcur with the release. A nonconcurrency will need a justification to support a recommendation for denial.

48.6.d. Disclosures

48.6.d.(1). Disclosures to record subjects are generally exempt from the requirements imposed by the Privacy Act. The Chief, FOIA/PA Office, is the primary Initial Denial Authority for the OIG DoD and is responsible for the release or denial of OIG DoD information requested under the provisions of the FOIA.

48.6.d.(2). Accounting for disclosures under the provisions of the FOIA is the sole responsibility of the Chief, FOIA/PA Office. The disposition of correspondence concerning disclosure of information from FOIA records is governed by the Federal Records Act of 1950, 44 U.S.C. 3101 *et seq.*

48.7. Privacy Act Requirements

48.7.a. **References.** Paragraphs 48.4.c., e., k., p., q.; 48.6.c.

48.7.b. **Statutory Requirement.** The Privacy Act imposes a statutory requirement that an accounting be maintained of all information disclosed from any system of records. This requirement pertains to information disclosed verbally, as well as in writing. It is the responsibility of the OIG DoD employee making the disclosure to ensure that proper disclosure accounting records are prepared.

48.7.c. **Disclosure of Personal Information to Other Agencies and Third Parties.** All PA requests received by DCIS field elements from individuals for personal information about themselves or other individuals (third parties) shall be forwarded to the FOIA/PA Office for further action. A copy of all responsive information being maintained by the DCIS field element must be included with the referral. The requester will be advised of the referral action by the DCIS field element (see **Attachments A and B**). Requests received by offices located at

Headquarters will be hand carried to the FOIA/PA Office. The same procedures will be carried out as established in paragraphs 48.6.c.(1). through (6).

48.7.d. **Disclosures Among DoD Components.** For the purpose of disclosure and disclosure accounting, DoD is considered a single agency.

48.7.e. **Disclosures Outside DoD.** Do not disclose personal information from a system of records outside DoD unless the release is for one of the specific nonconsensual purposes set forth below.

48.7.f. **Nonconsensual Disclosures**

48.7.f.(1). **Disclosures Within DoD**

48.7.f.(1).(a). Records pertaining to an individual may be disclosed without the consent of the individual to any DoD official who has need for the record in the performance of his/her assigned duties and has made a request in writing on Agency letterhead.

48.7.f.(1).(b). Rank, position, or title alone does not authorize access to personal information about others. An official need for the information must exist before a disclosure can be made.

48.7.f.(2). **Disclosures for Established Routine Uses**

48.7.f.(2).(a). DCIS records may be disclosed outside DoD without the consent of the individual to whom they pertain for an established routine use.

48.7.f.(2).(b). A routine use shall:

48.7.f.(2).(b).1. be compatible with and related to the purpose for which the record was compiled;

48.7.f.(2).(b).2. identify the person(s) or organization(s) to whom the record may be released;

48.7.f.(2).(b).3. identify, specifically, the uses to which the information may be put by the receiving agency;

48.7.f.(2).(b).4. have been published previously in the Federal Register.

48.7.f.(2).(c). A routine use must be established for each user of the information who needs official access to the records.

48.7.f.(2).(d). Blanket routine uses have been established for all OIG DoD-maintained systems of records (see **Attachment C**). Unless a system of records has been specifically excluded from a given blanket routine use, all blanket routine uses apply.

48.7.f.(2).(e). The written permission of the individual must be obtained if the recipient has not been identified in the Federal Register or a use to which the recipient intends to put the record has not been published in the system notice as a routine use.

48.7.f.(3). **Disclosure for Law Enforcement Purposes**

48.7.f.(3).(a). Records may be disclosed without the consent of the individual to whom they pertain to another agency or an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity, provided:

48.7.f.(3).(a).1. the civil or criminal law enforcement activity is authorized by law;

48.7.f.(3).(a).2. the head of the law enforcement activity or a designee has made a written request specifying the particular records desired and the law enforcement purpose (such as criminal investigation, enforcement of a civil law, or a similar purpose) for which the record is sought;

48.7.f.(3).(a).3. there is no Federal statute that prohibits the disclosure of the records.

48.7.f.(3).(b). Normally, blanket requests for access to any and all records pertaining to an individual are not honored.

48.7.f.(3).(c). A disclosure accounting must be maintained when a record is released to a law enforcement activity. The disclosure accounting shall not be made available to the individual to whom the record pertains if the law enforcement activity requests that the disclosure not be released.

48.7.f.(4). **Emergency Disclosures.** Records may be disclosed without the consent of the individual to whom they pertain if disclosure is made under compelling circumstances affecting the health or safety of any individual. The affected individual need not be the subject of the record disclosed. The DCIS field element receiving requests under these circumstances must contact the Chief, FOIA/PA Office, for additional instructions.

48.7.f.(5). **Disclosure to Congress.** Congressional inquiries received by DCIS elements should be forwarded to the Office of the Deputy Inspector General for Investigations (ODIG-INV) for action. (NOTE: Records may be disclosed without the consent of the individual to whom they pertain to either house of Congress or to any committee, joint committee, or subcommittee of Congress if the release pertains to a matter within the jurisdiction

of the committee. Any decision to make such a release is limited to the Inspector General; the Deputy Inspectors General; the Assistant Inspector General, Communications and Congressional Liaison; or the Initial Denial Authority under the provisions of the FOIA/PA.)

48.7.f.(6). Disclosure to the Government Accountability Office (GAO)

48.7.f.(6).(a). DCIS field elements may disclose DCIS records to GAO in the course of the activities of GAO.

48.7.f.(6).(b). A disclosure accounting must be made each time information is disclosed to GAO (see section 48.9.).

48.7.f.(7). Disclosures Under Court Orders

48.7.f.(7).(a). Records may be disclosed by a DCIS field element without the consent of the person to whom they pertain under a court order signed by a judge of a court of competent jurisdiction. Releases may also be made under the compulsory legal process of Federal or state bodies having authority to issue such process.

48.7.f.(7).(b). When a record is disclosed under this provision, make reasonable efforts to notify the individual to whom the record pertains, if the legal process is a matter of public record.

48.7.f.(7).(c). If the process is not a matter of public record at the time it is issued, seek to be advised when the process is made public and make reasonable efforts to notify the individual at that time.

48.7.f.(7).(d). Notification sent to the last known address of the individual, as reflected in the records, is considered reasonable effort to notify.

48.7.f.(7).(e). Make a disclosure accounting each time a record is disclosed under a court order or compulsory legal process (see section 48.9.).

48.7.f.(8). **Disposition of Records.** The Federal Records Act of 1950 governs the disposition of correspondence concerning disclosure of information from PA records.

48.8. Information Obtained From Financial Institutions

48.8.a. **References.** Paragraphs 48.4.a. and i., as implemented in Special Agents Manual (SAM) Chapter 14.

48.8.b. **Policy.** It is OIG DoD policy when obtaining financial records from a financial institution to seek the consent of the individual (customer) to whom the record pertains, unless doing so could compromise or harmfully delay a legitimate law enforcement inquiry. If the person declines to authorize Government access to his/her financial record, the alternative means

of obtaining the records authorized by the references cited in paragraph 48.8.a., as implemented in SAM Chapter 14, will be used.

48.8.c. **Special Provisions.** The provisions of the references cited in paragraph 48.8.a. do not govern obtaining access to financial records maintained by military banking contractors located outside the United States, in the District of Columbia, Guam, American Samoa, or the Virgin Islands. The procedures outlined in SAM Chapter 14 will be followed in obtaining financial information from these facilities.

48.8.d. **Disclosure Accounting.** Customer information obtained from financial institutions and disclosed in accordance with the provisions of the references cited and SAM Chapter 14 must be documented on DCIS Form 57 (see section 48.9. and Attachment D).

48.9. Disclosure Accounting

48.9.a. **References.** Section 48.4.

48.9.b. **Purpose.** The purpose of the PA accountability requirement is to allow individuals to determine to whom their records have been disclosed and to be able to advise the recipients of records of any disputed or corrected records.

48.9.c. **Disclosure Accounting.** Disclosure records must be prepared if the information disclosed is from either investigative or administrative files. A DCIS Form 57, Disclosure Accounting Sheet (Attachment D), will be prepared at the time the information is disclosed by the individual making the disclosure.

48.9.d. **Contents of Disclosure Accountings.** As indicated on DCIS Form 57, disclosure accountings shall contain:

48.9.d.(1). the date of the disclosure,

48.9.d.(2). a description of the information released,

48.9.d.(3). the purpose of the disclosure,

48.9.d.(4). the name and address of the person or agency to whom the disclosure was made.

48.9.e. **Accounting for Mass Disclosures.** When numerous similar records are released (such as transmittal of payroll checks to a bank), identify the category of records disclosed and include the data required in paragraph 48.9.d. in some form that can be used to construct an accounting disclosure record for individual records, if required.

48.9.f. **Disposition of Disclosure Accounting Records.** Disclosure accounting records are retained for 5 years after the disclosure, or the life of the record, whichever is longer. All

completed DCIS Forms 57 will be maintained in the case file. In lieu of Form 57, the memorandum provided by IOD pertaining to a FOIA request or release to an outside agency will be maintained in the case file.

48.9.g. Furnishing Disclosure Accounting to the Individual. The DCIS field element receiving requests from individuals for disclosure accountings should refer the requests to the Chief, FOIA/PA Office, for further action and advise the requester accordingly. Requests received by offices located at Headquarters will be hand carried to the FOIA/PA Office. The FOIA/PA Office will provide a copy of all disclosure accountings to the individual to whom the record pertains, except when:

48.9.g.(1). the disclosure has been made to a law enforcement activity, and the law enforcement activity has requested that disclosure not be made;

48.9.g.(2). the system of records has been exempted from the disclosure accounting requirement under an established exemption rule.

ATTACHMENTS

<u>Attachment</u>	<u>Title</u>
A	Sample Response to FOIA/PA Requester
B	Sample Referral Memorandum
C	OIG Blanket Routine Uses
D	Disclosure Accounting Sheet

ATTACHMENT A

SAMPLE RESPONSE TO FOIA/PA REQUESTER

(Requester's name and address)

Dear (requester's name):

This refers to your Freedom of Information Act (or Privacy Act) request of (date of request) seeking information concerning (brief summation of subject of request) that was received on (date received by FO/RA).

The information you seek is under the cognizance of the Chief, Freedom of Information Act and Privacy Act Office, Office of the Inspector General, Department of Defense. Your request has been forwarded to that official for further action and direct response to you.

Sincerely,

ATTACHMENT B

SAMPLE REFERRAL MEMORANDUM

MEMORANDUM FOR CHIEF, FOIA/PA OFFICE

SUBJECT: Freedom of Information Act (or Privacy Act) Request - (requester's name)

This office has received a Freedom of Information Act (or Privacy Act) request from (requester's name) seeking a copy of (subject of request) (Attachment 1).

The requester has been advised that his/her request was forwarded for your action and direct response. A copy of our response to the requester is provided as Attachment 2.

If you have any questions concerning this referral, please contact (name of FO/RA official most knowledgeable of the information requested) at (telephone number).

(Signature Block)

Attachments:

As stated

ATTACHMENT C

OIG BLANKET ROUTINE USES

Certain blanket “routine uses” of records have been established that are applicable to every record system maintained within the Department of Defense, unless specifically stated otherwise within a particular record system. These additional blanket routine uses of records are published below, only once, in the interest of simplicity, economy, and to avoid redundancy before the individual record system notices begin, rather than repeating them in every individual record system.

LAW ENFORCEMENT: In the event that a system of records maintained by this Component to carry out its functions indicates a violation or potential violation of law, whether civil, criminal, or regulatory in nature, and whether arising by general statute or by regulation, rule, or order issued pursuant thereto, the relevant records in the system of records may be referred, as a routine use, to the appropriate agency, whether Federal, state, local, or foreign, charged with the responsibility of investigating or prosecuting such violation or charged with enforcing or implementing the statute, rule, regulation, or order issued pursuant thereto.

DISCLOSURE WHEN REQUESTING INFORMATION: A record from a system of records maintained by this Component may be disclosed as a routine use to a Federal, state, or local agency maintaining civil, criminal, or other relevant enforcement information or other pertinent information, such as current licenses, if necessary to obtain information relevant to a component decision concerning the hiring or retention of an employee, the issuance of a security clearance, the letting of a contract, or the issuance of a license, grant, or other benefit.

DISCLOSURE OF REQUESTED INFORMATION: A record from a system of records maintained by this Component may be disclosed to a Federal agency in response to its request, in connection with the hiring or retention of an employee, the issuance of a security clearance, the reporting of an investigation of an employee, the letting of a contract, or the issuance of a license, grant, or other benefit by the requesting agency, to the extent that the information is relevant and necessary to the requesting agency’s decision on the matter.

CONGRESSIONAL INQUIRIES: Disclosure from a system of records maintained by this Component may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual. Coordinate with the Office of Communications and Congressional Liaison.

PRIVATE RELIEF LEGISLATION: Relevant information contained in all systems of records of DoD published on or before August 22, 1975, may be disclosed to the Office of Management and Budget (OMB) in connection with the review of private relief legislation as set forth in OMB Circular A-19, revised September 20, 1979, at any stage of the legislative coordination and clearance process as set forth in that circular.

DISCLOSURES REQUIRED BY INTERNATIONAL AGREEMENTS: A record from a system of records maintained by this Component may be disclosed to foreign law enforcement, security, investigatory, or administrative authorities in order to comply with requirements imposed by, or to claim rights conferred in, international agreements and arrangements, including those regulating the stationing and status in foreign countries of DoD military and civilian personnel.

DISCLOSURE TO STATE AND LOCAL TAXING AUTHORITIES: Any information normally contained in IRS Form W-2 that is maintained in a record from a system of records maintained by this Component may be disclosed to state and local taxing authorities with which the Secretary of the Treasury has entered into agreements pursuant to 5 U.S.C. 5516, 5517, and 5520, and only to those state and local taxing authorities for which an employee or military member is or was subject to tax regardless of whether tax is or was withheld. This routine use is in accordance with Treasury Financial Manual, Volume 3, Chapter 4000, April 2003.

DISCLOSURE TO THE OFFICE OF PERSONNEL MANAGEMENT: A record from a system of records subject to the Privacy Act and maintained by this component may be disclosed to the Office of Personnel Management (OPM) concerning information on pay and leave, benefits, retirement deductions, and any other information necessary for OPM to carry out its legally authorized Government-wide personnel management functions and studies.

DISCLOSURE TO THE DEPARTMENT OF JUSTICE FOR LITIGATION: A record from a system of records maintained by this Component may be disclosed as a routine use to any component of the Department of Justice for the purpose of representing the Department of Defense or any officer, employee, or member of the Department in pending or potential litigation to which the record is pertinent.

DISCLOSURE TO MILITARY BANKING FACILITIES OVERSEAS: Information as to current military addresses and assignments may be provided to military banking facilities that provide banking services overseas and are reimbursed by the Government for certain checking and loan losses. For personnel separated, discharged, or retired from the Armed Forces, information as to last known residential or home of record address may be provided to the military banking facility upon certification by a banking facility officer that the facility has a returned or dishonored check negotiated by the individual or the individual has defaulted on a loan and that if restitution is not made by the individual, the U.S. Government will be liable for the losses the facility may incur.

DISCLOSURE OF INFORMATION TO THE GENERAL SERVICES ADMINISTRATION: A record from a system of records maintained by this Component may be disclosed as a routine use to the General Services Administration (GSA) for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

DISCLOSURE OF INFORMATION TO THE NATIONAL ARCHIVES AND RECORDS ADMINISTRATION: A record from a system of records maintained by this Component may be disclosed as a routine use to the National Archives and Records

Administration (NARA) for the purpose of records management inspections conducted under authority of 44 U.S.C. 2904 and 2906.

DISCLOSURE TO THE MERIT SYSTEMS PROTECTION BOARD: A record from a system of records maintained by this Component may be disclosed as a routine use to the Merit Systems Protection Board, including the Office of the Special Counsel for the purpose of litigation, including administrative proceedings, appeals, special studies of the Civil Service and other merit systems, review of OPM or Component rules and regulations, investigation of alleged or possible prohibited personnel practices, including administrative proceedings involving any individual subject of a DoD investigation, and such other functions promulgated in 5 U.S.C. 1205 and 1206, or as may be authorized by law.

COUNTERINTELLIGENCE PURPOSES: A record from a system of records maintained by this Component may be disclosed as a routine use outside DoD or the U.S. Government for the purpose of counterintelligence activities authorized by U.S. law or Executive Order or for the purpose of enforcing laws that protect the national security of the United States.

ATTACHMENT D

DISCLOSURE ACCOUNTING SHEET

(Privacy Act of 1974, Public Law 93-579)
(DoD Directive 5400.11, "DoD Privacy Act Program")

Subject's full name, Social Security number, date of birth:

Recipient's name, agency, and address:

Purpose of disclosure (ROUTINE USE):

COPY PROVIDED: Yes No

Date of disclosure:

Description of material disclosed (Date of ROI and CCN. If disclosure was not total, identify information disclosed by paragraph number and identification of attachments.):

DCIS FORM 57

48-D-1

April 2011

CHAPTER 50

CASE REPORTING AND INFORMATION MANAGEMENT SYSTEM (CRIMS)

Contents	Section
Purpose	50.1
Authority	50.2
Responsibilities	50.3
Definitions	50.4
General Policies	50.5
Case Reporting Policy	50.6
Case Documents Policy	50.7
Subject Reporting Policy	50.8
Investigative Results Reporting Policy	50.9
Configuration Management	50.10
CRIMS Access	50.11

50.1. Purpose

50.1.a. This chapter provides policy guidance on reporting investigative and administrative data in CRIMS. It does not provide guidance on how to operate the system. For that information, consult the CRIMS user's manual, available in the CRIMS online help files, or contact the CRIMS Program Management Office.

50.1.b. CRIMS is the principal reporting system for timely reporting of DoD investigative activities. CRIMS helps the DoD OIG achieve its mission to support the warfighter; promote accountability, integrity, and efficiency; and advise the Secretary of Defense and Congress. CRIMS directly supports the OIG's statutory and regulatory reporting requirements, including the Semiannual Report to the Congress and the Council of Inspectors General on Integrity and Efficiency (CIGIE) Progress Report to the President. Consequently, CRIMS is a mission essential system, and ***the importance of accurate, timely, and complete data in the CRIMS cannot be overstated.***

50.1.c. CRIMS facilitates compliance with CIGIE's fourth qualitative standard for investigations, as published in CIGIE's "Quality Standards for Investigations," dated November 15, 2011, which states:

"Investigative data must be stored in a manner that allows effective retrieval, reference, and analysis, while ensuring the protection of sensitive data (i.e. personally identifiable, confidential, proprietary, or privileged information or materials). One of the many hallmarks of an efficient organization is its ability to retrieve information that it has collected. An effective information management system creates and enhances institutional memory. This, in turn, enhances the entire ability to conduct pattern and trend analyses and to fulfill the mandate of detection and prevention. Such a system also assists in making informed judgments relative to resource allocation, training needs, investigative program development, prevention activities, and implementation of

the investigative process. Further, the IG Act requires that certain data elements be reported in the semiannual reports to Congress.”

50.1.d. See Attachment A for the CRIMS mission and vision statement.

50.2. Authority

50.2.a. Authority to collect and report information in CRIMS is derived from the following.

50.2.a.(1). The Inspector General Act of 1978, as amended, 5 U.S.C. Appendix, Sections 2,4,5, and 8;

50.2.a.(2). DoD Directive (DoDD) 5106.01, “Inspector General of the Department of Defense,” dated April 20, 2012;

50.2.a.(3). DoD Instruction (DoDI) 5505.03, “Initiation of Investigations by Defense Criminal Investigative Organizations”, dated March 24, 2011;

50.2.a.(4). DoDI 5505.07, “Titling and Indexing Subjects of Criminal Investigations in the Department of Defense,” dated January 27, 2012;

50.2.a.(5). DoDD 7730.47, “Defense Incident-Based Reporting System,” dated January 23, 2014;

50.2.a.(6). DoDI 5525.16, “Law Enforcement Defense Data Exchange (LE D-DEx),” dated August 29, 2013;

50.2.a.(7). Executive Order 9397, “Numbering System for Federal Accounts Relating to Individual Persons” (as amended); and

50.2.a.(8). DoDI 2000.26, “Suspicious Activity Reporting,” dated November 1, 2011.

50.2.b. Privacy Act (PA) notices are not required pursuant to 5 U.S.C. 552a(e)(3) because an exemption rule for this record system has been promulgated in accordance with 5 U.S.C. 553(b)(1), (2), and (3), (c) and (e) and published in 32 CFR part 312. Therefore, DCIS personnel are not required to issue PA notices to individuals from whom personally identifiable information (PII) is collected.

50.3. Responsibilities

50.3.a. **Lead Agents.** Lead agents are DCIS personnel assigned as the lead agent on a particular investigation. Lead agents are the primary source of all investigative information entered into CRIMS and they, along with their managers, are ultimately responsible for the currency, accuracy, and completeness of data on their assigned cases reported in CRIMS.

50.3.b. Co-Case Agents. Co-case agents are assigned as such in CRIMS for a particular investigation. Co-case agents are responsible for timely, accurate, and complete reporting of all data from investigations to which they are assigned. All such reporting should be coordinated with the lead agent to avoid duplication and ensure appropriate reporting of investigative activities and results.

50.3.c. Office Administrative Staff. Office administrative staff are non-agent personnel who assist with reporting investigative and administrative information captured in CRIMS. They are not authorized to approve the opening or closure of case records or the validation of any investigative result in CRIMS on behalf of the case manager.

50.3.d. Case Managers. Case managers include special agents in charge (SACs), assistant special agents in charge (ASACs), and resident agents in charge (RACs). Case managers are responsible for ensuring the timely, accurate, and complete reporting of all data on investigations they supervise. Case managers are responsible for ensuring the integrity of information in CRIMS by periodically comparing CRIMS data with data in investigative reports and/or supporting documentation. Case managers will promptly coordinate investigative efforts between DCIS offices, including any needed transfers of open cases between offices. Case managers shall conduct all needed validation of CRIMS entries. Case managers shall request or concur with all requests to Internal Operations Directorate (INT) personnel to make material changes to CRIMS entries.

50.3.e. Desk Officers and Investigative Program Managers. Desk officers and investigative program managers shall be responsible for monitoring cases for which they have oversight responsibility, from case initiation through final closure, to ensure appropriate Headquarters visibility over significant investigative activity. Additionally, desk officers and/or program managers will assist in monitoring the integrity of information reported in CRIMS by periodically comparing CRIMS data with information captured in investigative reports and/or supporting documentation to help ensure timely, accurate, and complete reporting.

50.3.f. Internal Operations Directorate. INT shall be responsible for monitoring the integrity of information in CRIMS as well as answering all stakeholder inquiries, including those from DCIS executive leadership, the Inspector General, the Office of the Secretary of Defense, and Congress. INT will provide information necessary for the Semi-Annual Report to the Congress. INT will review appropriate investigative reports and other supporting documentation necessary to validate CRIMS entries. INT shall coordinate corrections and overriding changes to CRIMS when necessary.

50.3.g. Budget and Personnel. Budget and personnel staff shall be responsible for entry and update of all personnel-related data (e.g., new hires, separations, internal transfers, entrance-on-duty dates, separation dates, office assignments, etc.).

50.3.h. CRIMS Administrators. CRIMS administrators shall be responsible for administering the application, including maintaining system lookup lists, adding and removing users, and assigning user access permissions.

50.3.i. **CRIMS Program Manager.** The CRIMS program manager shall have overall responsibility for CRIMS policies and procedures stated in this chapter. The CRIMS program manager shall be responsible for validating all system-modification requirements. The CRIMS program manager shall assign CRIMS administrator responsibilities to DoD OIG personnel or contractors as appropriate. The CRIMS program manager shall review the CRIMS System of Records Notice every 2 years and update it as necessary, as required by IG Instruction 5400.11, “Privacy Act Program.”

50.3.j. **Information Systems Directorate.** The Information Systems Directorate (ISD) is responsible for providing technical support for CRIMS, including troubleshooting errors and modifying features to accommodate changing requirements. ISD will maintain the database, server infrastructure, reports, forms, scripts, and software packages, including software-license and maintenance agreements for the software components that make up the CRIMS application. ISD will provide enough network connectivity for DCIS offices to access CRIMS. ISD will ensure CRIMS meets standards for information assurance, consistent with DoD and OIG policies.

50.4. Definitions

50.4.a. See Attachment B for a list of CRIMS-related terms and their definitions.

50.5. General Policy

50.5.a. **Timely, Accurate, and Complete Reporting.** Responsible parties are required to enter appropriate data on *all* investigative activities in a timely, accurate, and complete manner consistent with the reporting timeframes established in SAM Chapter 28 (e.g., within 10 business days for information collected during case initiation, 5 business days for information collected during operational activities, etc.). This applies to *all* information collected in CRIMS. Consult the CRIMS data dictionary in Attachment C for a complete list of all core data tables and fields in CRIMS.

50.5.b. **Authority to Approve CRIMS Entries.** The authority for final approval of all CRIMS data entries rests with Internal Operations in consultation with Investigative and International Operations, as appropriate.

50.5.c. **External Reporting.** Official reporting of investigative results to stakeholders, such as the IG, OSD, and Congress, is particularly sensitive, and any misrepresentation could hinder the success of the OIG. The final version of any CRIMS data (other than investigative reports) *must* be approved by INT before it can be reported outside of DCIS, unless the information was obtained through pre-approved “canned” reporting mechanisms, such as providing input to the Semiannual Report to the Congress, responding to Congressional inquiries, supplying information for an official briefing, etc.

50.5.d. **Classified Investigations.** CRIMS is an unclassified system and, therefore, *only unclassified information can be collected in CRIMS*. At a minimum, a shell case record will be created to include the:

- 50.5.d.(1). unique identification number (UID),
- 50.5.d.(2). unclassified case title,
- 50.5.d.(3). case type,
- 50.5.d.(4). case category,
- 50.5.d.(5). lead agent,
- 50.5.d.(6). case office,
- 50.5.d.(7). case open date,
- 50.5.d.(8). DoD nexus (if unclassified),
- 50.5.d.(9). referral sources (if unclassified),
- 50.5.d.(10). priority investigation flag, and
- 50.5.d.(11). joint investigative agencies (if unclassified)

Consult SAM Chapter 28 or the DCIS National Security Program for further guidance on reporting classified investigative information.

50.6. Case Reporting Policy

50.6.a. Case Development Packages (CDPs). CDPs are the initial entries that lead to an open investigation/information report. They are intended to help agents collect information immediately before beginning an investigation/information report. CDPs may not remain open longer than 90 days without a note (made via the Initiation tab on the CRIMS Case form) indicating the CDP has been reviewed by the case manager. After the first 90 days, the CDP record must be reviewed every 30 days; this review should be noted on the Initiation tab until the case has been approved or the CDP has been disapproved. Consult SAM Chapter 28 for policy guidance on when a CDP should be converted to an open investigation/information report.

50.6.b. Duplicate Case Records. Duplicate case records are generally not permitted in CRIMS, because they can cause inaccurate reporting. A duplicate Case record occurs when a user creates a new record based on the same allegations as those being addressed under an existing Case record. For example, Office A opens a CRIMS Case record based on a *qui tam* referral also sent to Office B. If Office B later opens a CRIMS Case record based on the same allegations, it creates a duplicate Case record. In such instances, duplication of investigative results (e.g., the same indictment, conviction, and/or monetary recovery reported on multiple cases) and the splitting of results could degrade the accuracy of information reported to key stakeholders.

50.6.b.(1). One exception to the above policy is the existence of parallel criminal, civil, or administrative proceedings for which a prosecutor has ***expressly*** requested that DCIS pursue separate criminal and civil/administrative investigations ***under different case numbers***. Such circumstances are rare; there are many investigative tools that do not use grand jury proceedings. Moreover, the Department of Justice (DOJ) policy for coordinating parallel proceedings among DOJ attorneys recommends using investigative tools other than the grand jury to collect evidence in white-collar-crime cases. Other possible exceptions may be considered on a case-by-case basis.

50.6.b.(2). When such circumstances arise, the appropriate case manager will contact the CRIMS program office for guidance on how to initiate a duplicate CRIMS Case record. INT must approve the initiation of an otherwise duplicate CRIMS Case record before creating such a record in CRIMS.

50.6.b.(3). There is no need to create a duplicate CRIMS Case record to give credit to an agent or office outside the office of primary responsibility. Instead, use the “co-case agent” function in CRIMS to give full case credit to more than one agent. To give credit for individual investigative results or techniques, the “multiple credit agent” and “credit office” feature in CRIMS should be used. See CRIMS help resources for more information.

50.6.c. **Case Type.** Select the appropriate case type based on the following guidance:

50.6.c.(1). **Regular Investigation.** Regular investigations are the investigation of alleged criminal, civil, or administrative violations under the jurisdiction of DCIS or for which the Inspector General, or his/her designee, has directed DCIS to conduct an investigation. The full range of investigative techniques may be used in a regular investigation. Suspects associated with regular investigations are indexed in the Defense Central Index of Investigations (DCII) pursuant to DoD Instruction 5505.07, “Titling and Indexing of Subjects of Criminal Investigations in the Department of Defense.”

50.6.c.(2). **Information Report.** Information reports (IRs) are much more limited in scope than regular investigations and do not involve recording of arrests, seizures of Government property, or adjudicative referrals, actions, outcomes, or sentencing. An IR is used to document the receipt of information or to refer matters to other agencies or DCIS offices. IRs are opened and closed simultaneously and, therefore, cannot involve more than a few simple investigative techniques that do not require more than a short time to complete. Additionally, IRs cannot use certain invasive techniques, such as subpoenas, consensual/nonconsensual recordings, or covert operations. Furthermore, although IRs frequently do identify possible suspects, they do *not* result in the formal titling and indexing of those suspects. Nor do they report this information to the DCII, because IRs are limited in scope and do not normally develop enough information to meet the DoD standard for titling and indexing of subjects (i.e., “credible evidence” the suspect has committed a crime).

50.6.c.(3). **Investigative Project.** An investigative project is a proactive effort to identify areas where DoD is vulnerable to fraud or other criminal acts. Investigative projects do *not* involve the titling of suspects, but they may involve the identification and linkage of witnesses, victims, and/or targets. Investigative projects do not involve the recording of arrests, seizures of Government property, or adjudicative referrals, actions, outcomes, and/or sentencing actions.

50.6.c.(4). **Undercover Operation.**

(b)(7)(E)

(b)(7)(E)

50.6.c.(5). **Briefings.** Briefings are used to document mission briefings and other specialized briefings (e.g., Recovery Act–related briefings) provided by DCIS personnel to external entities. Briefings require that time charged to the specific effort be recorded for time-tracking purposes, as well as reporting the organization briefed and the numbers and types of personnel briefed.

50.6.c.(6). **External Lead Response.** DCIS responses to external lead requests (e.g., investigative lead requests received from non-DCIS agencies, such as the Military Criminal Investigative Organizations [MCIOs]) are special types of IRs. They are segregated from other IRs primarily because of special reporting requirements in the November 1997 MCIO Memorandum of Agreement (MOA). External lead responses do not involve adjudicative activities (e.g., adjudicative referrals, actions, outcomes, or sentencing activities). See SAM Chapter 28 for additional guidance regarding external lead reporting.

50.6.c.(7). **External Polygraph Support. NOTE: This case type is for use by Polygraph Program personnel only.** Polygraph support to external entities is tracked through this case type. Only Polygraph Program staff members should be creating polygraph support case types. The primary purpose of this case type is to track time spent in external polygraph support activities not directly related to a DCIS investigation.

50.6.b.(9). **General Computer Forensics Support. NOTE: This case type is for use by computer forensics personnel only.** The primary purpose of this case type is to track time spent in general computer forensics support not directly related to a DCIS investigation.

50.6.c.(10). **General Technical Investigative Support. NOTE: This case type is for use by Technical Services personnel only.** The primary purpose of this case type is to track time spent in general technical investigative support not directly related to a DCIS investigation.

50.6.c.(11). **Inspection.** For Headquarters and Office of Quality Assurance and Standards (QAS) use only.

50.6.c.(12). **Management Inquiries.** For Headquarters use only.

50.6.c.(13). **QAS Information Report.** For QAS use only.

50.6.c.(14). **QAS Internal Investigation.** For QAS use only.

50.6.d. **Case Title.** The case title field in CRIMS will contain the name of the primary suspect or the appropriate impersonal or generic title, as specified in SAM Chapter 28. See SAM Chapter 28 for guidance on titling subjects in investigative reports and on formatting case titles.

50.6.e. **Referral Source(s) (formerly known as “Originating Agency”).** Referral source(s) include referrals from other agencies as well as internal sources (e.g., spin-off cases from projects and UCOs, IRs referred from other DCIS offices, etc.). Referral sources include *all* referrals, regardless of whether they were received before or after case initiation. At least one referral source *must* be specified in CRIMS for each case record where the case type is one of the following:

- 50.6.e.(1). regular investigation,
- 50.6.e.(2). information report,
- 50.6.e.(3). investigative project, or
- 50.6.e.(4). UCO.

Additionally, certain referral sources are identified in SAM Chapter 28 as agencies for which numbered referrals must be tracked. Agency tracking numbers for cases that involve a referral from one of these agencies must be entered in CRIMS as soon as feasible to ensure timely, accurate, and complete stakeholder reporting. See SAM Chapter 28 for more information about agencies involving numbered referrals.

50.6.f. **Spin-Off Cases.** Spin-off cases are those stemming from a DCIS regular investigation, IR, investigative project, or UCO. Spin-off cases will be identified as such by specifying the referral source as follows:

50.6.f.(1). “DCIS” when the source of the information is a DCIS Regular Investigation or IR;

50. 6.f.(2). “PROJSPN” when the source of the information is a DCIS Investigative Project; and

50. 6.f.(3). “UCOSPN” when the source of the information is a DCIS UCO.

The UID of the case *must* be entered in the Agency Tracking Number field in order to maintain traceability for all spin-off cases.

50.6.g. **DoD Nexus.** At least one DoD nexus *must* be specified in CRIMS where the case type is one of the following:

- 50.6.g.(1). regular investigation;
- 50.6.g.(2). information report,
- 50.6.g.(3). investigative project, or
- 50.6.g.(4). UCO.

The DoD nexus consists of the following three elements:

- 50.6.g.(6). DoD component,
- 50.6.g.(7). DoD subcomponent, and
- 50.6.g.(8). unit description.

DoD component and subcomponent are **required** fields. DoD component is linked directly to the DoD organization chart. DoD subcomponent identifies the subcomponent of the DoD component affected by the alleged wrongdoing. Unit description is an optional, free-text field that lets users list a unit-level description for the DoD subcomponent affected by the alleged conduct. For example, Defense Logistics Agency (DLA) is a DoD component, Disposition Services is a subcomponent under DLA, and Disposition Services Site–Richmond is a possible description to identify the unit level of the DoD entity affected by the alleged wrongdoing.

50.6.h. **Case Category.** A case category **must** be assigned to the following case types:

- 50.6.h.(1). regular investigation,
- 50.6.h.(2). information report,
- 50.6.h.(3). investigative project, or
- 50.6.h.(4). UCO.

If a case can be defined under more than one case category, the single most appropriate or highest-priority category must be entered in the CRIMS case record. If later information indicates a different case category should be assigned, the case category shall be promptly changed, and the basis for the change should be documented in the online documents/Virtual Case File. Case category is an important factor in reporting the nature of DCIS cases to key stakeholders, including the IG, the Secretary of Defense, and Congress. Therefore, it is critical that case categories be accurately assigned and maintained in CRIMS. Although lead agents and/or case managers initially determine the appropriate case category, desk officers and program managers are ultimately responsible for ensuring that case records in CRIMS are properly categorized. Additionally, INT personnel are responsible for monitoring the quality of information stored in CRIMS and, accordingly, may require that the case category be changed to more accurately reflect the true nature of the allegations under investigation.

50.6.i. **Estimated Loss.** Estimated loss **must** be entered relative to all case records where the case type is one of the following:

- 50.6.i.(1). regular investigation,
- 50.6.i.(2). information report,
- 50.6.i.(3). investigative project, or
- 50.6.i.(4). UCO.

An estimated or alleged loss to the U.S. Government should be identified at case opening. CRIMS is programmed to enter a default value of “\$0.” However, an estimated dollar loss should be entered, **to the nearest whole dollar**, by the lead agent or case manager as soon as it is

known. If a reliable source later provides information that alters the original estimated loss, the lead agent or case manager should update the estimate. For example, if the allegations involve a \$100,000 contract, and the loss to the Government is \$50,000, then \$50,000 should be entered as the estimated dollar loss (not the entire \$100,000). In cases where no dollar loss is expected or it is impossible to determine, leave the \$0 entry in this field. Keep in mind that this figure is just an estimate based on the information available at the time it is entered and is based on the user's subjective assessment of the facts. The user need not obtain objective evidence to support this figure before making an entry. However, the estimate should be reasonable and based on information documented in the Case Initiation Report or other investigative report available in the CRIMS VCF.

50.6.j. **Priority Cases.** Priority case criteria apply to the following case types:

- 50.6.j.(1). regular investigation, and
- 50.6.j.(2). UCO.

Priority investigations are chosen based on criteria set in an annual investigative priorities document prepared and distributed by DCIS executive leadership.

50.6.k. **Headquarters Approval to Upgrade Certain Cases to Priority Investigations.**

For certain case categories to be upgraded, DCIS executive leadership requires Headquarters approval, based on additional criteria. In such cases, the case manager should coordinate with the appropriate desk officer/program manager. See the annual DCIS investigative priorities guidance for more information. To update CRIMS, Internal Operations must be promptly notified that Headquarters has approved the upgrade.

50.6.l. **Special Interest Cases (SICs).** SIC criteria may apply to all case records where the case type is one of the following:

- 50.6.l.(1). regular investigation,
- 50.6.l.(2). information report,
- 50.6.l.(3). investigative project, or
- 50.6.l.(4). UCO.

SAM Chapter 28 specifies the criteria for determining which cases are considered SICs. CRIMS *must* be updated promptly when the agent receives information indicating one or more SIC criteria apply to an open investigation.

50.6.m. **Joint Investigative Agencies.** This designation can apply to the following case types:

- 50.6.m.(1). regular investigation,
- 50.6.m.(2). investigative project, and
- 50.6.m.(3). UCO.

For each joint investigative agency, its case number, the date it joined our investigation, and (if appropriate) the date joint efforts ceased **must** be entered in CRIMS.

50.6.n Case Disposition. Case disposition applies to the following case types:

- 50.6.n.(1). regular investigation,
- 50.6.n.(2). information report,
- 50.6.n.(3). investigative project, and
- 50.6.n.(4). UCO.

The final disposition of cases must be recorded before the transfer or closure of an investigation, or before a case is placed in “suspense” in CRIMS. SAM Chapter 28 discusses appropriate case dispositions.

50.6.o. eGuardian/LESARS. DoDI 2000.26, “Suspicious Activity Reporting,” establishes DoD policy, assigns responsibilities, and prescribes procedures for the documentation, storage, and exchange of suspicious activity reports (SARs) through law enforcement channels to improve the protection of DoD personnel, facilities, and forces in transit. DCIS agents receiving information about suspicious activities will record such information and the results of any preliminary investigative activity in an information report (IR) and place the IR in CRIMS for tracking purposes.

50.7. Case Documents Policy

50.7.a. Investigative Reports. SAM Chapter 28 defines investigative reports as documents “written to record information gathered during an investigative activity, such as an interview, record review, search and arrest warrants, or surveillance.” At a minimum, the following investigative reports **must** be uploaded to the VCF, unless there is a compelling reason to keep the report off-line:

- 50.7.a.(1). case initiation reports,
- 50.7.a.(2). information reports,
- 50.7.a.(3). case summary reports,
- 50.7.a.(4). reports of investigation,
- 50.7.a.(5). interview reports,
- 50.7.a.(6). significant incident reports (including any supporting documentation),
and
- 50.7.a.(7). audit coordination memorandum/fraud vulnerability

Reports received from joint investigative agencies and incorporated into the official case file should be uploaded into the VCF unless the authoring agency’s policy expressly prohibits this. Reports generated from certain databases, including, but not limited to, the National Crime Information Center (NCIC), Financial Crimes Enforcement Network (FinCEN), and Treasury Enforcement Communications System (TECS) will not be placed in the VCF. Consult SAM Chapter 28 for additional guidance.

50.7.b. **Attachments.** Attachments to investigative reports should be uploaded to the VCF where appropriate and practical. However, good judgment should be used when determining whether to upload an attachment to the VCF. Users should keep in mind that storage space is finite and should refrain from uploading unnecessary files. A general rule of thumb is that the file size should not be larger than 15 megabytes. In any event, all attachments *must* be referenced in the report and relevant information from the attachment *must* be summarized in the report if the attachment has not been uploaded to the VCF.

50.7.c. **Complete Case File.** Although only the above reports are required to be uploaded to the VCF, the intent of the VCF is to provide a comprehensive collection of all case reports and attachments that is fully indexed and keyword searchable. *DCIS personnel should make full use of the VCF and load all investigative reports and appropriate attachments.*

50.7.d. **Text-Searchable/OCR Format.** All documents uploaded to the VCF *must* be in text-searchable/OCR (optical character recognizable) format. Scanned documents may need to be converted into OCR format before uploading to the VCF. Adobe Acrobat Pro software includes tools for converting documents into OCR format. For assistance, consult the help files in Adobe Acrobat Pro or contact the CRIMS program office.

50.7.e. **UCO Documents.** Access to documents associated with an undercover operation will be restricted to the lead agent, case managers, office administrative staff, special operations program managers, CRIMS administrators, and the SharePoint administrator in the Information Systems Directorate. However, note that documents associated with UCO spin-off investigations are not restricted access.

50.7.f. **Excluded Documents.** Certain investigative reports and other documents may need to be excluded from the VCF. For example, if the case manager believes there is a compelling reason to keep a report offline, he or she will contact the CRIMS program manager. The CRIMS program manager will coordinate the request with the appropriate desk officer/program manager for his or her concurrence. The CRIMS program manager will communicate concurrence or nonconcurrence to the requesting case manager via e-mail, and the lead agent, case manager, or office administrator will place a generic Form 1 in the VCF with the following statement:

“This [type of report] is not available in this system. Please contact [name of lead agent] for more information.”

Similarly, certain reports and documents *must* be excluded:

- 50.7.f.(1). reports containing classified information;
- 50.7.f.(2). reports containing information about matters occurring before the grand jury;
- 50.7.f.(3). Bank Secrecy Act Suspicious Activity Reports;
- 50.7.f.(4). Treasury Enforcement Communications System printouts; and
- 50.7.f.(5). other restricted-dissemination reports.

50.7.g. **Corrected Investigative Reports.** If an approved version of an investigative report must be rewritten or any type of change/edit made, both the corrected and original copies *must* be uploaded to CRIMS. Refer to SAM Chapter 28 for “Corrected” Form 1 procedures.

50.7.h. **Digital Signatures.** All DCIS-issued investigative reports uploaded to the VCF *must* be digitally signed by the case manager who approved the final version of the report. The case manager’s digital signature is necessary to ensure the version of the report uploaded to the VCF is the management-approved final version.

50.7.i. **Timeliness.** Investigative reports and related attachments should be uploaded to the VCF within 10 business days of the date the report was approved.

50.8. Subject Reporting Policy

50.8.a. **DCII Reporting.** The Defense Central Index of Investigations (DCII) is an automated central index that identifies investigations by DoD investigative agencies and personnel-security determinations by DoD adjudicative authorities. DCIS is required to report information about “suspects” to DCII in accordance with DoDI 5505.07.

50.8.b. **Subject Classification.** CRIMS uses the term “subject” to refer to four different classes of individuals and entities associated with investigations: suspects, victims, witnesses, and targets. It is important to note that CRIMS uses “suspect” to refer to the person or entity suspected of wrongdoing, whereas other references (e.g., DoD policy documents) use “subject” to refer to the person or entity suspected of wrongdoing.

50.8.b.(1) **Suspect.** Suspects will be titled in accordance with DoDI 5505.07, which states, “Titling and indexing in the DCII shall be done as soon as the investigation determines that credible information exists that the subject committed a criminal offense.” DoDI 5505.07 defines “credible information” as:

“information disclosed or obtained by a criminal investigator that, considering the source and nature of the information and the totality of the circumstances, is sufficiently believable to lead a trained criminal investigator to presume that the fact or facts in question are true.”

Titling a suspect in a regular investigation in CRIMS triggers a report to DCII. However, titling a suspect in IRs does *not* result in a report to DCII, because IRs generally do not contain “credible information...that the subject committed a criminal offense.”

Suspect records may only be associated with the following case types:

- 50.8.b.(1).a. regular investigations; and
- 50.8.b.(1).b. information reports.

50.8.b.(2). **Target.** Use the “target” classification to identify subjects for whom “credible information [does not yet exist] that the subject committed a criminal offense” and for whom the “witness” or “victim” classification does not apply. For example, a

person of interest, whose involvement in the alleged conduct is not yet known, should be classified as a “target” in CRIMS. Targets are ***not*** reported to DCII.

50.8.b.(3). **Victim.** Use the “victim” classification to identify an individual, business, government entity, or other organization that “has suffered direct physical, emotional, or pecuniary harm as a result of the commission of a crime” (42 U.S.C. 10607[e][2]).

50.8.b.(4). **Witness.** Use the “witness” classification to identify an individual or organization that is not a victim as defined in 50.8.b.(3). above and may provide information about the alleged wrongdoing.

50.8.c. **Removal of Subject Information from CRIMS.** Normally, subject information will not be removed from CRIMS unless there is a compelling reason to do so. If a subject record needs to be removed from CRIMS, the appropriate case manager will send to the CRIMS program manager an e-mail identifying the case and subject record(s) at issue and the specific reason(s) for removing the subject record(s) from CRIMS. Each request will be considered on a case-by-case basis. If a request is approved, the removal of the subject record will be coordinated with the DCIS DCII administrator for removal of the subject’s information from DCII.

50.8.d. **Subject Type.** Subject type identifies subjects as “individuals,” “businesses,” “government,” “financial,” or “religious organization,” in accordance with DoDD 7730.47.

50.8.e. **Top 100 DoD Contractors.** Each year, the top 100 DoD contractors are identified in various forums, based on the total DoD procurement dollars provided to that contractor during the specified fiscal year. The appropriate user will flag a suspect in CRIMS as a Top 100 contractor when the contractor has been identified on the list of Top 100 DoD contractors for 1 or more fiscal years during which the alleged wrongdoing occurred. CRIMS does not automatically flag suspect records as Top 100. If the suspect was not on the Top 100 list for at least 1 fiscal year during which the alleged wrongdoing occurred, the suspect will not be flagged as a Top 100 contractor.

50.9. Investigative Results Reporting Policy

50.9.a. Investigative results include the following:

50.9.a.(1). Adjudicative referrals for criminal, civil, and administrative action;

NOTE: The Inspector General Act (5 U.S.C. App., Section 4[d]) requires the Inspector General to “report expeditiously to the Attorney General whenever the Inspector General has reasonable grounds to believe there has been a violation of Federal criminal law.” This is accomplished through referral of criminal matters to a U.S. Attorney’s Office and/or DOJ. Additionally, 5 U.S.C., App., Section 8(d) requires the Inspector General of the Department of Defense to “expeditiously report suspected or alleged violations of chapter 47 of title 10, United States Code (Uniform Code of Military Justice), to the

Secretary of the military department concerned or the Secretary of Defense.”
This is accomplished by coordinating with the appropriate MCIO.

50.9.a.(2). Adjudicative actions (e.g., Federal indictments, civil complaints, administrative charges, etc.; see Attachment E for complete list of actions.)

NOTE: Criminal complaints are not reported in CRIMS because complaints are preliminary charges pending formal indictment or information. Superseding charges are not reported in CRIMS. Only the initial indictment, information, or state charge should be reported. However, per SAM Chapter 28, all significant events, such as superseding charges must be reported via the appropriate Form 1.

50.9.a.(3). Adjudicative outcomes (e.g., conviction, conviction of a lesser offense, acquittal, administrative outcome, etc.; see Attachment E for complete list of outcomes.)

50.9.a.(4). Adjudicative sentencing actions (e.g., confinement, fine, probation, restitution, suspension/debarment from contracting, etc.; see Attachment E for complete list of sentencing actions.)

50.9.a.(5). Recovered Government property (i.e., stolen/illegally converted Government property of value that has been returned to the Federal Government and does **not** include property seized relative to asset forfeiture proceedings); and

50.9.a.(6). Arrests.

50.9.b. The investigative results entered into CRIMS must be the outcome of the involvement of DCIS investigators in the investigation. Investigative results obtained by other agencies or through administrative means not involving DCIS cannot be claimed.

50.9.c. **Dates.** See Attachment F for guidance on the dates that should be reported relative to the various types of investigative results.

50.9.d. **Adjudicative Referral Acceptance/Declination.** Adjudicative referrals **must** be entered into CRIMS anytime a referral has been made. An adjudicative referral is considered “accepted” for CRIMS purposes if the matter has been formally referred for possible criminal, civil, or administrative action and the receiving agency has not formally declined to take action. Formal referral can include written and/or verbal submissions to an outside agency to take action. For example, if a lead agent has an ongoing dialogue with an Assistant U.S. Attorney (AUSA) about a possible criminal or civil prosecution relative to a particular open investigation, and the dialogue causes the AUSA grand jury to issue subpoenas, make civil investigative demands, or otherwise take action to further the investigation, then for CRIMS purposes, the matter has been “accepted” for possible prosecution. If the matter is later declined for prosecution, CRIMS should be updated to change the earlier acceptance to a declination.

50.9.e. Validation of Investigative Results. All investigative results *must* be validated in accordance with Attachment E. Validation of investigative results *must* include review of the appropriate supporting documentation. Results that have not yet been validated will not be reported to key stakeholders (e.g., Congress, Secretary of Defense, Inspector General, etc.).

50.9.f. Cost Adjustment. Cost adjustments involve a well-documented and specific reduction in contract price that the Government would otherwise be required to pay a contractor if the cost adjustment had not been made. An example of a cost adjustment is Government contracting officer's issuance of a contract modification that results in a specified reduction in contract price as a result of a contractor's failure to provide materials or services that met the contract specification. This type of cost adjustment may be claimed as a reportable significant incident if it is the result of investigative efforts by DCIS.

50.9.g. Cost Avoidance. Cost avoidance is "[a]n action taken in the immediate time frame that will decrease costs in the future" (Source: Glossary of Defense Acquisition Acronyms and Terms (<https://dap.dau.mil/glossary/pages/1674.aspx>)). Because cost avoidance is not normally well-documented or specific as to the exact cost avoided, DCIS senior management has decided that DCIS does not claim cost avoidance as a reportable significant incident.

50.9.h. Proceeds. Refers to monies received or acquired by a Federal law enforcement agency that has statutory authority to receive such monies during a joint authorized undercover operation. Proceeds are used to offset necessary and reasonable expenses (a determination made by the joint agency) incurred during an authorized undercover operation. DCIS may report in CRIMS the total amount of "proceeds" received by the joint Federal investigative agency after DCIS has initiated a spin-off investigation. "Proceeds" are separate and distinct from "seizures" and must be clearly identified on supporting documentation (Forms 1, Memorandums for the Record, other agency reports, etc.). Seizure reporting (administrative/civil/criminal) policy is in SAM Chapter 3. Contact the Asset Forfeiture Program for any questions/clarification on the reporting of seizures relative to forfeiture actions.

50.9.i. Entry and Disclosure of Sealed Adjudicative Data. CRIMS allows for entry of sealed adjudicative data (e.g., charging actions, outcomes, and sentencing actions). DCIS personnel *must* diligently ensure that any sealed adjudication data are properly flagged in CRIMS as "Sealed" to prevent unauthorized disclosure. Any disclosure of a record that was not properly flagged is the responsibility of the user who failed to properly flag the record. Additionally, all CRIMS users *must* ensure they do not improperly disclose information about sealed adjudicative data that have been recorded in CRIMS. Any disclosure of data that were properly flagged is the responsibility of the user who made the disclosure and must be promptly reported to the CRIMS program manager. Finally, DCIS personnel *must* report when information has been unsealed by unchecking the "Sealed" box. Only unsealed statistics will be validated.

50.9.j. Reporting of Juvenile Proceedings. See SAM Chapter 22, Juveniles and Criminal Investigations, for requirements for the protection and release of information on juveniles.

50.9.k. Reporting the Value of Recovered Government Property. When reporting the dollar value of recovered Government property, DCIS personnel must act prudently to establish estimated values. Ultimately, the information entered into CRIMS must be defensible relative to reporting investigative results to the Inspector General, Secretary of Defense, and/or Congress.

50.9.k.(1). DCIS personnel should rely primarily on third-party documentation, such as current appraisals or official Government documents reporting the current value of the item(s) recovered. However, when no such formal documentation exists, DCIS personnel, in establishing the value of recovered Government property, must be conservative and carefully consider the totality of the circumstances.

50.9.k.(2). In all cases, DCIS personnel must provide a clearly documented, sound rationale for establishing the value of the item(s) recovered, in the form of a Significant Incident Report and include any supporting documentation, such as third-party documentation and/or photographs that help convey the current value and condition of the property.

50.9.k.(3). Consider the following scenario in which careful consideration and a conservative approach are needed to establish the value of recovered property.

DCIS personnel have recovered an F-4 aircraft originally purchased in 1963 for \$10,000,000 (the acquisition value). It no longer has no wings, avionics, or engines. DLA Disposition Services (formerly the Defense Reutilization Service) has issued a DD-1348 indicating the plane's value is \$2,000,000. Investigation has revealed the basis for that value was a comparison with a similar but flightworthy aircraft the Navy was going to use for target practice. The investigation found the subject bought the item in a recent private-party sale for \$10,000. The conservative, prudent, and defensible amount to claim in this scenario is \$10,000, based on the recent fair-market transaction and absent any third-party documentation indicating the amount paid was not the true, fair-market value of the aircraft.

50.9.l. Conflict-of-Interest Referrals. Per SAM Chapter 28, conflict-of-interest referrals involving a violation of 18 U.S.C. §§ 203, 205, 207, 208, and/or 209 by an executive branch employee must be reported to the Office of Government Ethics (OGE). Accordingly, adjudicative referral records in CRIMS involving conflict-of-interest violations *must* be flagged as OGE-reportable. See SAM Chapter 28, Investigative Reports, for further guidance on reporting conflicts of interest to OGE.

50.9.m. Investigative Techniques. Techniques are not tracked for reporting to key external stakeholders (e.g., Congress, Secretary of Defense, etc.). Data on investigative techniques are used primarily for internal oversight of investigative activity in a particular investigation. Consult your RAC for further guidance.

50.10. Configuration Management

50.10.a. Configuration management is the process of managing requested changes to the CRIMS application so that beneficial changes can be implemented over time while avoiding negative consequences. CRIMS is a complex software application with many interrelated parts that address a wide range of stakeholder requirements. A change to one part of the application can have unintended consequences for other parts. Additionally, there are limited resources to develop and implement changes to the application. Formal configuration management procedures help ensure efficient use of those resources.

50.10.b. All requests for changes to CRIMS application(s) must be processed under the configuration management procedures addressed in Attachment G.

50.11. CRIMS Access

50.11.a. Access to CRIMS is restricted to DoD OIG personnel and contractors with a verified need to know. Appropriate due diligence will be performed by the CRIMS PMO to validate all requests for CRIMS access before access is granted.

50.11.b. All agents (i.e., series 1811s, including case managers, desk officers, and program managers), administrative support assistants, investigative review specialists, and investigative analysts will automatically be granted access to CRIMS based on a presumed need to know as a result of their verified positions and duties. The level of access will be determined by their assigned positions and will be consistent with business rules for the CRIMS-related functions of those positions.

50.11.c. Access to CRIMS by OIG personnel and contractors other than those in positions specifically mentioned in 50.11.b. above will be considered on a case-by-case basis.

50.11.c.(1). Personnel employed or managed directly by DCIS (e.g., interns and contractors) will be granted access to CRIMS based on a digitally signed e-mail submitted to the CRIMS PMO at INV-CRIMS-Help@dodig.mil by the appropriate supervisor, identifying the person's name, position, and general duties as they relate to the request for CRIMS access. In the case of contractor personnel, the e-mail will be submitted by the appropriate DCIS point of contact for that contract. The CRIMS PMO will independently verify the person's position, document verification results, and grant access based on the supervisor's certification of the need to know.

50.11.c.(2). OIG personnel and contractors not employed or managed directly by DCIS may be granted access to CRIMS only with approval from the Deputy Inspector General for Investigations (DIGI). The appropriate supervisor will send a digitally signed e-mail to the CRIMS PMO at INV-CRIMS-Help@dodig.mil, identifying the person's name, position, and general duties as they relate to the request for CRIMS access. In the case of contractor personnel, the e-mail will be submitted by the appropriate contracting officer's representative or component POC. The CRIMS PMO will verify the information in the request and formally submit the request to the DIGI for

approval. Once DIGI approves it, the CRIMS PMO will document the approval and grant the requested access.

50.11.d. Delegation of Case Manager Role. When necessary, case manager roles may be delegated to other CRIMS users based on a digitally signed e-mail from the RAC or SAC/ASAC to the CRIMS PMO at INV-CRIMS-Help@dodig.mil. Based on the e-mail, the CRIMS PMO will delegate the appropriate role as requested and document the details of the delegation.

ATTACHMENTS

Attachment	Title
A	CRIMS Mission and Vision Statement
B	Data Dictionary
C	Definitions
D	Current Adjudicative Data Types
E	Validation of Investigative Results
F	Configuration Management Procedures

ATTACHMENT A

CRIMS MISSION AND VISION

As of March 20, 2014

This document describes the current mission and vision concerning the Case Reporting and Information Management System (CRIMS) and will guide future decisions relative to CRIMS development, deployment, and user training activities. On March 20, 2014, the DCIS Information Technology Working Group (ITWG), made up of headquarters and field personnel, considered three key factors supporting the CRIMS vision and voted unanimously to approve each of the following decisions:

- Decision 1 - Adopt the full CRIMS integration model
- Decision 2 - Make use of COTS tools to the maximum extent possible, and
- Decision 3 - Make agents responsible for CRIMS data input.

CRIMS Mission:

Serve as the principal reporting system for timely reporting of investigative activities relevant to the Department of Defense that supports the warfighter; promotes accountability, integrity, and efficiency; and advises the Secretary of Defense and Congress.

CRIMS Vision:

CRIMS directly supports the Inspector General's statutory and regulatory reporting requirements, including the Semiannual Report to Congress and the CIGIE Progress Report to the President.

CRIMS will be continually developed and refined to fully support the investigative process through such features as unified reporting (i.e., simultaneous preparation of investigative reports and collection of key data in the structured database) and electronic processing of investigative support requests (e.g., lead requests, communication intercept authorizations, etc.).

CRIMS will maximize return on investment through the use of commercial-off-the-shelf (COTS) technology while minimizing negative impacts on DCIS mission accomplishment. Where compelling factors exist, custom-developed approaches may be implemented to meet mission requirements, but normally only after COTS solutions have been considered and eliminated as viable solutions.

Agent personnel will be the primary source of all investigative information entered into CRIMS and they along with their managers will ultimately be responsible for the currency, accuracy, and completeness of data reported in CRIMS relative to their assigned cases.

☒ Approved/ ☐ Disapproved

BURCH.JAMES.B.1385
207219

James B. Burch
Deputy Inspector General
for Investigations

Digitally signed by BURCH.JAMES.B.1385207219
DN: c=US, o=U.S. Government, ou=DoD, ou=PKI,
ou=DODIG, cn=BURCH.JAMES.B.1385207219
Date: 2014.04.28 09:25:31 -0400

Date

ATTACHMENT B

CRIMS DATA DICTIONARY

The following table provides a high-level summary of the core data tables in CRIMS:

DATA TYPE	DESCRIPTION	CUSTOM TABLES	CUSTOM FIELDS
CASE (Tables 1 – 26)	Data that primarily pertain to the overall investigative effort (e.g., Case Title, Case Category, Estimated Dollar Loss, Joint Investigative Agencies, Investigative Techniques, etc.)	26	163
SUBJECT (Tables 27 – 34)	Data that primarily pertain to specific suspects, victims, witnesses, or targets (i.e., persons of interest)—e.g., name, address, other identifying information, etc.	8	79
RESULTS (Tables 35 – 45)	Data that primarily pertain to investigative results (i.e., referrals, charging actions, outcomes, sentencing, arrests, and recovered Government property)	11	144
TOTAL		45	386

The following tables explain each CRIMS custom data table and the custom fields showing the core data used for investigative oversight and reporting.

TABLE 1: CASE

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
NONE	Captures general details about the Case record.	44

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
1	APPROVAL STATUS	Used to facilitate approval workflow for the following case types: REGI, INFO, and PROJ	PICKLIST	
2	APPROVAL STATUS (DISPLAY)	Identifies the current Approval Status for all Case Types. NOTE: All “approval status” fields are copied to this field to display the current approval status for ALL case records.	NVARCHAR	100
3	ARE OCO COUNTRIES INVOLVED	Identifies whether the case involves Overseas Contingency Operations countries. Consult International Operations for guidance.	PICKLIST	
4	ASSET FORFEITURE FLAG	Identifies whether the case involves potential asset forfeiture action. Consult the Asset Forfeiture Program for guidance.	PICKLIST	

CUSTOM FIELDS (Case Table cont'd):

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
5	AVERAGE EVALUATION RATING	Applies only to briefings where category is "Mission Briefing (Recovery Act)." Records the average evaluation rating from participants in this type of briefing activity.	NVARCHAR	100
6	BRIEFING CATEGORY	Applies only to briefings. Identifies the briefing category.	LOOKUP	
7	BRIEFING CITY	Applies only to briefings whose category is "Mission Briefing (Recovery Act)" or "Outreach (Recovery Act)." Identifies the city where the briefing happened.	NVARCHAR	100
8	BRIEFING DATE	Applies only to briefings. Identifies the date the briefing activity occurred.	DATE/TIME	
9	BRIEFING STATE	Applies only to briefings for which the category is "Mission Briefing (Recovery Act)" or "Outreach (Recovery Act)." Identifies the state the briefing happened in.	LOOKUP	
10	CASE CATEGORY	Identifies the case category as specified in SAM Chapter 28.	LOOKUP	
11	CASE CLOSE DATE	System-generated. Identifies the date the Case record was approved for closure in CRIMS.	DATE/TIME	
12	CASE DISPOSITION	Identifies the current status of the case. Normally populated at time of case closure.	LOOKUP	
13	CASE OPEN DATE	System-generated. Identifies the date the Case Development Package (CDP) record was approved as a Case record in CRIMS.	DATE/TIME	
14	CASE TYPE	Identifies the type of Case record, consistent with SAM Chapter 50 requirements.	LOOKUP	
15	CDP CLOSE DATE	System-generated. Identifies the date the CDP record was closed in CRIMS.	DATE/TIME	
16	CDP OPEN DATE	System-generated. Identifies the date the CDP record was created in CRIMS.	DATE/TIME	
17	CREATED BY	System-generated. Identifies the user who created the record.	LOOKUP	

CUSTOM FIELDS (Case Table cont'd):

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
18	CREATED ON	System-generated. Identifies the date the record was created.	DATE/TIME	
19	DESK OFFICER	System-generated. Identifies the name of the desk officer who approved initiation of the Case record.	LOOKUP	
20	DESK OFFICER APPROVAL REQUIRED	System-generated. Identifies Case records where that require desk-officer approval.	BIT	
21	DESK OFFICER DATE APPROVED	System-generated. Identifies the date the desk officer approved the Case record.	DATE/TIME	
22	EGUARDIAN/LESARS	Identifies Information Reports involving information reported to eGuardian as an LE Suspicious Activity Report (LESARS)	PICKLIST	
23	ESTIMATED DOLLAR LOSS	Identifies estimated dollar loss as defined in SAM Chapter 50.	MONEY	
24	GROUP 1 UCO APPROVAL STATUS	Used to facilitate approval workflow for UCO case types where classification is "Group 1"	PICKLIST	
25	GROUP 2 UCO APPROVAL STATUS	Used to facilitate approval workflow for UCO Case Types where classification is "Group 2"	PICKLIST	
26	LEAD AGENT	Identifies the agent to whom the case is currently assigned.	LOOKUP	
27	NUMBER OF ATTENDEES	Applies to briefings only. Shows the number of attendees at the briefing.	INT	
28	OFFICE	Identifies the DCIS office to which the case is currently assigned.	LOOKUP	
29	OPEN STATUS	System-generated. Identifies the current open status of the Case record.	PICKLIST	
30	PRESENTATION WITH OTHER OIGs	Applies to briefings whose category is "Outreach (Recovery Act)." Identifies briefings given with other OIGs.	BIT	
31	PRIORITY INVESTIGATION FLAG	Identifies whether the case is considered a priority investigation. Set automatically based on case category and estimated dollar loss (where applicable) but can be overridden by authorized case manager.	BIT	

CUSTOM FIELDS (Case Table cont'd):

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
32	PRIORITY OVERRIDE DATE	System-generated. Identifies the date the Priority Investigation Flag was manually overridden by a case manager.	DATE/TIME	
33	PRIORITY OVERRIDE MANAGER	System-generated. Identifies the name of the case manager who manually overrode the Priority Investigation Flag.	LOOKUP	
34	PRIORITY OVERRIDE NOTE	Identifies the reason for the manual override of the Priority Investigation flag.	NTEXT	500
35	REVIEWED FOR S&D	Identifies Case records that have been reviewed by the HQ coordination of remedies program manager for possible suspension and/or debarment action.	YES/NO	
36	SHAREPOINT DOCUMENT LIBRARY URL	System-generated. Identifies the SharePoint URL of the folder where documents linked to this case record are stored.	NVARCHAR	255
37	STAFF PREP TIME	Applies to briefings whose category is "Mission Briefing (Recovery Act)." Identifies the total hours spent preparing for the briefing.	NVARCHAR	100
38	TARGET AUDIENCE	Applies to briefings whose category is "Mission Briefing (Recovery Act)." Identifies the target audience for the briefing.	LOOKUP	
39	TIMETRACKING APPROVAL STATUS	Used to facilitate approval workflow for case types TECH, CFOR, and POLY.	PICKLIST	
40	TITLE	Case title. Should identify primary subject or impersonal/generic title consistent with SAM Chapter 28 requirements.	NVARCHAR	100
41	TOTAL TRAINING TIME	Applies to briefings whose category is "Mission Briefing (Recovery Act)." Lists the total time attributed to the briefing.	NVARCHAR	100
42	TRAINING LENGTH	Applies to briefings whose category is "Mission Briefing (Recovery Act)." Identifies the time the training took.	NVARCHAR	100

CUSTOM FIELDS (Case table cont'd):

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
43	UCO Classification	Only applies to UCO case type. Identifies the UCO classification (Group 1 or Group 2).	PICKLIST	
44	UID Number	The 10-digit number assigned to the Case record at creation.	NVARCHAR	10
44	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 2: CASE ACCESSED LOG

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
CASE	Date, time, and identity of all users, EXCEPT the lead agent who accessed the Case record. Triggers an e-mail alert to the lead agent if he/she has opted to receive them.	3

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
45	CASE	System-generated. Identifies the parent Case record this record is associated with.	LOOKUP	
46	DATE ACCESSED	System-generated. Identifies the date and time the Case record was accessed by the specified user.	DATE/TIME	
47	USER	System-generated. Identifies the user who accessed the parent Case record.	LOOKUP	
3	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 3: CASE ACTIVITY SUMMARY

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
CASE	Captures information on activities in connection with the parent Case record. This is an optional table users may use to track investigative activities.	3

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
48	ACTIVITY DATE	Date activity was completed	DATE/TIME	
49	AGENT	Name of person performing the activity	LOOKUP	

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
50	CASE	Identifies parent Case record the activity is associated with	LOOKUP	
3	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 4: CASE AGENTS

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
CASE	Captures information about co-case agents assigned to Case records.	4

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
51	AGENT	Identifies the agent assigned as co-case agent for the parent Case record	LOOKUP	
52	CASE	System-generated. Identifies the parent Case record.	LOOKUP	
53	CASE AGENT TYPE	Identifies the case agent type (e.g., co-case agent)	LOOKUP	
54	EFFECTIVE DATE	Identifies the effective date the agent was assigned as co-case agent relative to the parent case record.	DATE/TIME	
4	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 5: CASE CONTACTS

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
CASE	Links Case records to Contact records.	2

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
55	CASE	System-generated. Identifies the parent Case record this record is associated with.	LOOKUP	
56	CONTACT	Identifies the Contact record associated with the parent Case record	LOOKUP	
2	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 6: CASE CONTRACTS

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
CASE	Captures information about contracts associated with the parent Case record.	24

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
57	CASE	System-generated. Identifies the parent Case record this record is associated with.	LOOKUP	
58	CONTRACT DESCRIPTION	Provides general description of the goods/services procured relative to this contract.	NTEXT	2,000
59	CONTRACT NUMBER	Identifies the contract number.	NVARCHAR	100
60	CONTRACT OFFICE CITY	Identifies the city of the contracting office.	NVARCHAR	100
61	CONTRACT OFFICE COUNTRY	Identifies the country of the contracting office.	LOOKUP	
62	CONTRACT OFFICE DODAAC	Identifies the DODAAC of the contracting office.	NVARCHAR	100
63	CONTRACT OFFICE NAME	Identifies the name of the contracting office.	NVARCHAR	100
64	CONTRACT OFFICE STATE	Identifies the state the contracting office is in.	LOOKUP	
65	CONTRACTOR ADDRESS 1	Identifies the contractor's street address.	NVARCHAR	100
66	CONTRACTOR ADDRESS 2	Identifies the contractor's street address.	NVARCHAR	100
67	CONTRACTOR CAGE CODE	Identifies the contractor's CAGE code.	NVARCHAR	100
68	CONTRACTOR CITY	Identifies the city the contractor is in.	NVARCHAR	100
69	COUNTRACTOR COUNTRY	Identifies the country the contractor is in.	LOOKUP	
70	CONTRACTOR NAME	Identifies the name of the contractor.	NVARCHAR	100
71	CONTRACTOR PHONE NUMBER	Identifies the contractor's phone number.	NVARCHAR	100
72	CONTRACTOR STATE	Identifies the state where the contractor is located.	LOOKUP	
73	CUSTOMER CITY	Identifies the city where the buying activity is.	NVARCHAR	100
74	CUSTOMER COUNTRY	Identifies the country where the buying activity is.	LOOKUP	

CUSTOM FIELDS (Case Contracts table cont'd):

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
75	CUSTOMER DODAAC	Identifies the DODAAC of the buying activity.	NVARCHAR	100
76	CUSTOMER NAME	Identifies the name of the buying activity.	NVARCHAR	100
77	CUSTOMER STATE	Identifies the state where the buying activity is.	LOOKUP	
78	DUNS NUMBER	Identifies the contractor's DUNS number.	NVARCHAR	100
79	EFFECTIVE DATE	The effective date of the contract.	DATE/TIME	
80	TOTAL AMOUNT	The total dollar value of the contract.	MONEY	
24	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 7: CASE COUNTRIES

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
CASE	Captures country information associated with the parent Case record.	2

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
81	CASE	System-generated. Identifies the parent Case record this record is associated with.	LOOKUP	
82	COUNTRY	The country the parent Case record is related to.	LOOKUP	
2	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 8: CREDIT CARD FRAUD

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
CASE	Captures information about Government credit cards involved in alleged fraud relative to the parent Case record.	2

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
83	CASE	System-generated. Identifies the parent Case record this record is associated with.	LOOKUP	

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
84	CREDIT CARD FRAUD TYPE	The type of Government credit card involved in alleged fraud.	LOOKUP	
2	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 9: CASE DOCUMENTS

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
CASE	Captures information about case documents uploaded into the VCF.	5

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
85	CASE	System-generated. Identifies the parent Case record.	LOOKUP	
86	DATE OF DOCUMENT	Identifies the date of the document uploaded.	DATE/TIME	
87	DESCRIPTION	Presents the user-supplied description of the document uploaded.	NVARCHAR	100
88	DOCUMENT TYPE	Identifies the document type.	LOOKUP	
89	DOCUMENT URL	System-generated. Document URL (i.e., hyperlink to the document record stored in SharePoint.	NVARCHAR	255
5	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 10: CASE INVESTIGATIVE TECHNIQUES

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
CASE	Captures information about investigative techniques performed relative to the parent Case record.	6

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
90	ADDITIONAL COMMENTS	Free-text field for the user to make general comments on the investigative technique.	NTEXT	500
91	CASE	System-generated. Identifies the parent Case record this record is associated with.	LOOKUP	
92	DATE PERFORMED	The date the technique was performed.	DATE/TIME	

CUSTOM FIELDS (Case Investigative Techniques table cont'd):

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
93	INVESTIGATIVE TECHNIQUE	Lookup field that identifies the specific technique performed relative to the parent Case record.	LOOKUP	
94	QUANTITY	The total instances of the specified technique performed on the date indicated.	INT	
95	UID Number	System-generated. The UID number assigned to the parent Case record.	NVARCHAR	10
6	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 11: COMPUTER CRIMES

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
CASE	Captures information about computer crimes activities associated with the parent Case record.	8

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
96	CASE	System-generated. Identifies the parent Case record this record is associated with.	LOOKUP	
97	DAMAGE DONE	Indicates whether the incident resulted in damage to the network/domain affected by intrusion incident.	BIT	
98	DATE AND TIME OF INCIDENT	Date and time of incident	DATE/TIME	
99	EXPLOIT	Identifies type of exploit involved	LOOKUP	
100	INCIDENT CATEGORY	Identifies incident category	LOOKUP	
101	REMEDIATION/PATCH PUBLISHED OR ZERO DAY EXPLOIT	Not used.	NVARCHAR	255
102	REPORT NUMBER	The number of the report published by the reporting agency	NVARCHAR	20
103	REPORT TYPE PUBLISHED	Identifies the report type published by the agency that reported the incident	LOOKUP	
8	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 12: COMPUTER CRIMES SUBJECT

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
COMPUTER CRIMES	Captures information about subjects associated with a Computer Crimes parent record	2

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
104	COMPUTER CRIME	Identifies the Computer Crimes parent record to which this record is associated.	LOOKUP	
105	SUBJECT	Identifies the Subject record this record is associated with.	LOOKUP	
2	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 13: DESTINATION COUNTRY

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
TECHNOLOGY PROTECTION	Captures information about destination countries associated with the parent Technology Protection record.	2

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
106	COUNTRY	Identifies the country to which the USML article(s) is/are being shipped.	LOOKUP	
107	TECHNOLOGY PROTECTION	Identifies the parent Technology Protection record this record is associated with.	LOOKUP	
2	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 14: DOD NEXUS

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
CASE	Identifies the DoD agency(ies) affected by the allegations being investigated relative to the parent Case record	4

CUSTOM FIELDS (DoD Nexus table cont'd):

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
108	CASE	System-generated. Identifies the parent Case record this record is associated with.	LOOKUP	
109	DoD Component	Identifies the top-level DoD Component (the DoD organization chart-level component) affected by the allegations associated with the parent Case record.	LOOKUP	
110	DoD Subcomponent	Identifies the working-level component affected by the allegations associated with the parent Case record ((i.e., the component directly affected by the alleged wrongdoing).	LOOKUP	
111	Unit Description	Optional. User-specified unit description of the lowest level of the DoD subcomponent affected by the alleged wrongdoing. The intent of this field is to enable local managers to identify DoD activities in the local AOR who are affected by DCIS investigations.	NTEXT	2,000
4	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 15: JOINT AGENCY

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
CASE	Captures information about agencies who are actively working the investigation jointly with DCIS.	6

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
112	AGENCY	Identifies the joint investigative agency associated to the parent Case record.	LOOKUP	
113	AGENCY POINT OF CONTACT	Optional. Identifies the agency POC.	NVARCHAR	
114	AGENCY TRACKING NUMBER	Identifies the joint agency tracking number (i.e., case number).	NVARCHAR	
115	CASE	System-generated. Identifies the parent Case record to which this record is associated.	LOOKUP	

CUSTOM FIELDS (Joint Agency table cont'd):

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
116	END DATE	Identifies the date the joint agency terminated its joint investigation.	DATE/TIME	
117	START DATE	Identifies the date the joint agency began its joint investigation.	DATE/TIME	
6	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 16: ORIGINATING AGENCY

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
CASE	Identifies official source(s) of information for the allegations being investigated relative to the parent Case record. Includes all formal numbered referrals, regardless of when they were received.	6

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
118	AGENCY	Identifies the agency that referred the information that led to or supported the ongoing investigation.	LOOKUP	
119	AGENCY TRACKING NUMBER	Identifies the tracking number used by the referring agency.	NVARCHAR	100
120	CASE	System-generated. Identifies the parent Case record to which this record is associated.	LOOKUP	
121	DATE UNSEALED	Applies only to <i>qui tam</i> referrals from Department of Justice (DOJ). Identifies the date the <i>qui tam</i> complaint was unsealed by the court.	DATE/TIME	
122	SEALED	Applies only to <i>qui tam</i> referrals from DOJ. Identifies whether the <i>qui tam</i> complaint is currently under seal.	BIT	
123	UNSEALING AUTHORITY	Identifies the authority that unsealed the <i>qui tam</i> complaint (e.g., "U.S. District Court, Eastern District of VA").	NVARCHAR	100
6	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 17: PRODUCT SUBSTITUTION

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
CASE	Captures product substitution information associated with the parent Case record.	8

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
124	CASE	System-generated. Identifies the parent Case record which this record is associated with.	LOOKUP	
125	COMMON COMMODITY NAME	Identifies the common name describing the part affected by the alleged product substitution/nonconforming part.	NVARCHAR	100
126	CRITICAL APPLICATION ITEM	Identifies whether the part is a critical application item.	BIT	
127	END USE DESCRIPTION	Describes the end use application(s) for the parts involved (e.g., F-16 aircraft, Bradley Fighting Vehicle, etc.)	NVARCHAR	255
128	FLIGHT SAFETY CRITICAL APPLICATION PART	Identifies whether the part is a flight safety critical application part.	BIT	
129	MANUFACTURER NAME	Identifies the manufacturer's that produced the part.	NVARCHAR	100
130	MANUFACTURER PART NUMBER	Identifies the manufacturer's part number.	NVARCHAR	20
131	NATIONAL STOCK NUMBER	Identifies the national stock number assigned to the part.	NVARCHAR	20
8	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 18: RECOVERY ACT

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
CASE	Captures Recovery Act agency information associated with the parent Case record.	3

CUSTOM FIELDS (Recovery Act table cont'd):

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
132	CASE	System-generated. Identifies the parent Case record to which this record is associated.	LOOKUP	
133	DOD COMPONENT	Identifies top-level DoD component affected by the Recovery Act-related investigation	LOOKUP	
134	DOD SUBCOMPONENT	Identifies the working-level DoD component affected by the Recovery Act-related investigation.	LOOKUP	
3	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 19: RECOVERY ACT PROJECT/CONTRACT

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
RECOVERY ACT PROJECT/CONTRACT	Captures information about Recovery Act projects and/or contracts associated with a Recovery Act RA Program parent record.	6

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
135	ACTUAL LOSS	Identifies the actual loss (vs. estimated loss) determined through investigation of Recovery Act-related investigation.	MONEY	
136	CONTRACT AWARD AMOUNT	Identifies the award amount associated with the Recovery Act contract award.	MONEY	
137	CONTRACT NUMBER	Identifies the contract number associated with the Recovery Act contract.	NVARCHAR	100
138	ESTIMATED LOSS	Identifies the estimated loss associated with the specified Recovery Act contract and/or project.	MONEY	
139	RECOVERY ACT PROJECT/CONTRACT NAME	Identifies the Recovery Act project or contract name.	NVARCHAR	100
140	RECOVERY ACT RA PROGRAM	Identifies the Recovery Act RA Program parent record the record is associated with.	LOOKUP	
6	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 20: RECOVERY ACT RA PROGRAM

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
RECOVERY ACT	Captures information about the Recovery Act program associated with the parent Recovery Act record.	2

CUSTOM FIELDS (Recovery Act RA Program table cont'd):

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
141	RECOVERY ACT	System-generated. Identifies the Recovery Act parent record this record is associated with.	LOOKUP	
142	RECOVERY ACT PROGRAM	Identifies the Recovery Act program affected by the alleged conduct.	LOOKUP	
2	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 21: RECOVERY ACT REFERRAL

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
RECOVERY ACT	Captures information about referrals made to other agencies relative to a Recovery Act parent record.	2

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
143	REFERRAL DATE	Identifies the date the Recovery Act referral was made to another agency.	DATE/TIME	
144	REFERRAL METHOD	Identifies how the referral was made.	LOOKUP	
2	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 22: SPECIAL INTEREST FACTORS

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
CASE	Identifies the special interest case (SIC) factors associated with the parent Case record.	2

CUSTOM FIELDS (Special Interest Factors table cont'd):

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
145	CASE	System-generated. Identifies the parent Case record to which this record is associated.	LOOKUP	
146	SPECIAL INTEREST	Identifies the special interest factor that applies to the parent Case record	LOOKUP	
2	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 23: SUSPECTED PRODUCT IRREGULARITY REPORTS

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
CASE	Captures information about suspected product irregularity reports (SPIRs) issued relative to the parent Case record.	6

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
147	CASE	System-generated. Identifies the parent Case record the record is associated with.	LOOKUP	
148	GIDEP	Identifies information about the Government-Industry Data Exchange Program alert issued (if applicable).	NVARCHAR	100
149	MANUFACTURER	Identifies the manufacturer of the suspected irregular part.	NVARCHAR	100
150	PRODUCT	Identifies the name/description of the product.	NVARCHAR	100
151	SAFETY SEQUENCE NUMBER	Number assigned by HQ for tracking of SPIR.	NVARCHAR	100
152	SAFETY VALIDATION	Identifies the safety validation related to the SPIR.	LOOKUP	
6	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 24: TECHNICAL ASSISTANCE

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
CASE	Captures information about technical assistance requests (e.g., requests for laboratory examination, DCAA audit support, etc.) submitted to external agencies relative to the parent Case record.	5

CUSTOM FIELDS (Technical Assistance table cont'd):

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
153	ACCEPT	Indicates whether the outside agency accepted the technical assistance request.	BIT	
154	AGENCY	Identifies the outside agency whose technical assistance was requested.	LOOKUP	
155	CASE	System-generated. Identifies the parent Case record the record is associated with.	LOOKUP	
156	REMARKS	General remarks on the technical assistance request.	NTEXT	2,000
157	REQUEST DATE	The date the technical assistance request was submitted to the outside agency.	DATE/TIME	
5	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 25: TECHNOLOGY PROTECTION

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
CASE	Captures technology protection information associated with the parent Case record.	4

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
158	CASE	System-generated. Identifies the parent Case record this record is associated with.	LOOKUP	
159	END USE DESCRIPTION	Identifies the end use description (e.g., "F-16 aircraft") for the US Munitions List (USML) item involved.	NVARCHAR	255
160	USML ARTICLE DESCRIPTION	Identifies the specific USML article description in the International Traffic in Arms Regulation.	LOOKUP	
161	USML ARTICLE NOMENCLATURE	Free-text field for user to provide a custom description for the USML article.	NVARCHAR	100
4	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 26: TRANSSHIPMENT COUNTRIES

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
TECHNOLOGY PROTECTION	Captures information about the transshipment countries associated with the parent Technology Protection record.	2

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
162	COUNTRY	Identifies the country through which the USML article is being shipped to its final destination.		
163	TECHNOLOGY PROTECTION	Identifies the parent Technology Protection record this record is associated with.	LOOKUP	
2	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 27: CASE SUBJECTS

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
CASE	Captures information about subjects associated with the parent Case record.	46

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
164	ADDRESS TYPE	Identifies the address type (e.g., home, work, other) for Primary Address fields.	LOOKUP	
165	ALIEN REGISTRATION NUMBER	Identifies the alien registration number associated with the subject.	NVARCHAR	100
166	ALLEGATION STATUS	Founded, Unfounded, or Unresolved	PICKLIST	
167	BRANCH OF SERVICE	Identifies the military branch of Service for military members	LOOKUP	
168	CASE	Identifies the parent Case record to which the Subject record is associated.	LOOKUP	
169	CITY	Identifies the city of the subject's primary address.	NVARCHAR	100
170	CITY OF BIRTH	Subject's city of birth.	DATE/TIME	
171	CLASSIFICATION	Suspect, witness, victim, target (i.e., person of interest)	LOOKUP	
172	COMPANY DIVISION	Name of company division (used for non-person subjects)	NVARCHAR	100

CUSTOM FIELDS (Case Subjects table cont'd)

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
173	COMPANY GROUP	Name of company group (used for non-person subjects)	NVARCHAR	100
174	COUNTRY	The country of the subject's primary address	LOOKUP	
175	COUNTRY OF BIRTH	The country where the subject was born	LOOKUP	
176	DATE ADDED	Date subject record was added to the subject table. (Carried over from legacy system [IDS] because IDS did not have a "Created On" field and we could not modify the Created On field in CRM.)	DATE/TIME	
177	DATE CLASSIFIED AS SUSPECT	The date the subject was classified as a "suspect." This is user-specified, and this field was added at the field's request relative to the "Target Database" requirement.	DATE/TIME	
178	DATE OF BIRTH	Subject's date of birth	DATE/TIME	
179	DRIVERS LICENSE NUMBER	Subject's driver's license number	NVARCHAR	20
180	EDUCATION	Subject's education level	NVARCHAR	100
181	EMPLOYER	Subject's employer	NVARCHAR	200
182	ETHNICITY	Subject's ethnicity	LOOKUP	
183	FIRST NAME	Subject's first name	NVARCHAR	100
184	FOREIGN ID NUMBER	Subject's foreign ID number (used in conjunction with ID Designator)	NVARCHAR	100
185	FUGITIVE	Identifies subject as a fugitive	BIT	
186	FUNCTION	Identifies subject's job function	LOOKUP	
187	GENDER	Subject's gender	LOOKUP	
188	GOVERNMENT RELATIONSHIP	Identifies subject's relationship to the Federal Government	LOOKUP	
189	ID DESIGNATOR	Specifies the type of primary identification recorded in one of the following fields * SSN* Foreign ID * Alien Registration Number	LOOKUP	
190	INDUSTRY	Identifies subject's industry	LOOKUP	
191	JUVENILE	System-generated based on comparison of system date and date of birth. Indicates whether subject was a juvenile when the record was created.	BIT	
192	LAST NAME	Subject's last name	NVARCHAR	100

CUSTOM FIELDS (Case Subjects table cont'd)

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
193	LICENSE ISSUE STATE	Identifies the state of issue for subject's driver's license	LOOKUP	
194	MIDDLE NAME	Subject's middle name	NVARCHAR	100
195	MILITARY RANK	Military member's rank	LOOKUP	
196	ORGANIZATION NAME	Organization/business name	NVARCHAR	100
197	PAY GRADE	Subject's pay grade (for military and Federal civilian employees)	LOOKUP	
198	RACE	Subject's race	LOOKUP	
199	SSN	Subject's SSN	NVARCHAR	100
200	STATE	The state where the subject's primary address is	LOOKUP	
201	STATE OF BIRTH	State where subject was born	LOOKUP	
202	STREET ADDRESS 1	Street address (1) where subject's primary location	NVARCHAR	100
203	STREET ADDRESS 2	Street address (2) where subject's primary location	NVARCHAR	100
204	STREET ADDRESS 3	Street address (3) where subject's primary location	NVARCHAR	100
205	SUFFIX	Subject's name suffix (e.g., Jr, Sr., III, etc.)	LOOKUP	
206	TOP 100 COMPANY	Indicates whether the subject is a DoD Top 100 contractor.	BIT	
207	TYPE	Identifies subject type (e.g., Individual, Business, Government, etc.)	LOOKUP	
208	UID Number	System-generated. The UID number assigned to the parent Case record.	NVARCHAR	10
209	ZIP CODE	The zip code of the subject's primary address	NVARCHAR	10
46	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 28: ALIAS IDENTIFICATION

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
CASE SUBJECT	Captures information about aliases associated with subject	4

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
210	FIRST NAME	Alias first name used by subject	NVARCHAR	30
211	LAST NAME	Alias last name used by subject	NVARCHAR	30

CUSTOM FIELDS (Alias Identification table cont'd)

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
212	MIDDLE NAME	Alias middle name used by subject	NVARCHAR	30
213	SUBJECT	Identifies the parent Case Subject record to which the alias identification elements associated.	LOOKUP	
4	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 29: IP ADDRESSES

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
CASE SUBJECT	Captures information about IP addresses associated with subject.	4

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
214	COMPUTER CRIME	Identifies the parent Computer Crimes record the IP address is associated with.	LOOKUP	
215	IP ADDRESS	The IP address	NVARCHAR	15
216	SUBJECT	Identifies the parent subject record the IP address is associated with.	LOOKUP	
217	TYPE	Identifies the type of IP address	LOOKUP	
4	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 30: LAW ENFORCEMENT RECORDS CHECKS

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
CASE SUBJECT	Captures information about law enforcement records checks associated with subject.	2

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
218	SUBJECT	Identifies the parent record to which the law enforcement records check is associated	LOOKUP	
219	SUMMARY	Summary of results of LE records check	NTEXT	2,000
2	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 31: OTHER ADDRESSES

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
CASE SUBJECT	Captures information about addresses other than the primary address associated with the subject.	9

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
220	ADDRESS TYPE	Identifies the address type (e.g., Home, Work, Other)	LOOKUP	
221	CITY	Identifies the city of the address.	NVARCHAR	100
222	COUNTRY	Identifies the country of the address.	LOOKUP	
223	STATE	Identifies the state of the address.	LOOKUP	
224	STREET ADDRESS 1	Identifies the street address of the location.	NVARCHAR	100
225	STREET ADDRESS 2	Identifies the street address.	NVARCHAR	100
226	STREET ADDRESS 3	Identifies the street address.	NVARCHAR	100
227	SUBJECT	Identifies the parent subject record this record is associated with.	LOOKUP	
228	ZIP CODE	Identifies the zip code of the subject address.	NVARCHAR	10
9	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 32: PHONE NUMBERS

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
CASE SUBJECT	Captures information about all phone numbers associated with the subject	4

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
229	PHONE NUMBER	Identifies the phone number associated with the parent subject record.	NVARCHAR	15
230	PHONE TYPE	Identifies the phone type (e.g., home, cell, work, other, etc.).	LOOKUP	
231	SUBJECT	Identifies the parent subject record this phone number is associated with.	LOOKUP	

CUSTOM FIELDS (Phone Numbers table cont'd)

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
232	US/INTERNATIONAL	Identifies whether the phone number is a U.S. or international number.	LOOKUP	
4	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 33: PHOTOGRAPHS

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
CASE SUBJECT	Captures photographs associated with the subject.	2

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
233	CRIMS SUBJECT	Identifies the parent subject record to which this record is related		
234	PHOTOGRAPH DESCRIPTION	Describes photographs attached to the record. Each photo is attached as a note.	NVARCHAR	100
2	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 34: SECONDARY IDENTIFICATION

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
CASE SUBJECT	Captures information about secondary identifications (e.g., alternate SSNs, passports, alternate driver's licenses, etc.) associated with subject	6

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
235	COUNTRY	Identifies the country from which a foreign ID was issued.	LOOKUP	
236	ID NUMBER	Identifies the number of the ID.	NVARCHAR	25
237	ISSUING AUTHORITY	Identifies the agency that issued the ID.	NVARCHAR	100
238	OTHER ID TYPE	Identifies the ID Type (e.g., , Driver's' License, Passport, etc.).	LOOKUP	
239	STATE	Identifies the state where the ID was issued.	LOOKUP	

CUSTOM FIELDS (Secondary Identifications table cont'd)

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
240	SUBJECT	Identifies the parent subject record to which the Secondary ID record is associated.	LOOKUP	
6	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 35: ADJUDICATIVE ACTIONS

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
ADJUDICATIVE REFERRAL	Captures information about adjudicative actions (i.e., criminal, civil, or administrative charging actions) relative to the parent adjudicative referral record.	16

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
241	ACTION DATE	Identifies the date the adjudicative action occurred or was filed.	DATE/TIME	
242	ADJUDICATIVE ACTION TYPE	Identifies the action type (e.g., Federal indictment, information, civil complaint, administrative charge, etc.)	LOOKUP	
243	ADJUDICATIVE REFERRAL	Identifies the parent adjudicative referral record the record is associated with.	LOOKUP	
244	ADJUDICATIVE REFERRAL TYPE	Identifies the referral type (i.e., criminal, civil, or administrative)	LOOKUP	
245	CASE	Identifies the Case record with which the action record is associated.	LOOKUP	
246	DATE VALIDATED	Identifies the date the action record was validated	DATE/TIME	
247	REFERRAL AGENCY	Identifies the referral agency.	LOOKUP	
248	REFERRAL DATE	Identifies the referral date.	DATE/TIME	
249	SAR PERIOD REPORTED	Identifies the SAR period during which the action was reported.	NVARCHAR	8
250	SAR REPORTABLE	Indicates whether the action is considered SAR reportable.	BIT	
251	SEALED	Indicates whether the Action was filed under seal.	BIT	
252	SUBJECT	Identifies the subject record the action record is associated with.	LOOKUP	

CUSTOM FIELDS (Adjudicative Actions table cont'd)

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
253	UID NUMBER	Identifies the UID number of the Case record with which the action record is associated with.	NVARCHAR	10
254	UNSEALING AUTHORITY	Identifies the unsealing authority (i.e., the person or entity that authorized the unsealing of the court record) relative to the action.	NVARCHAR	100
255	VALIDATED BY	Identifies the name of the person who validated the action.	LOOKUP	
256	VALIDATION STATUS	Identifies the current validation status (i.e., pending validation, submitted for validation, or validated).	LOOKUP	
16	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 36: ADJUDICATIVE OUTCOME VIOLATIONS

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
ADJUDICATIVE OUTCOME	Captures information about violations associated with the parent Adjudicative Outcome record.	10

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
257	ADJUDCIATIVE OUTCOME	Identifies the parent Adjudicative Outcome record	LOOKUP	
258	CASE	Identifies the Case record this Adjudicative Outcome Violation record is associated with.	LOOKUP	
259	CFR VIOLATION	Identifies the CFR violation associated with the parent Outcome record.	LOOKUP	
260	COUNT	Identifies the number of counts	INT	
261	OTHER VIOLATIONS	Identifies other violations (i.e., not USC, USCMJ, or CFR violations).	NTEXT	2000
262	SUBJECT	Identifies the Subject record this Adjudicative Outcome Violation record is associated with.	LOOKUP	
263	UCMJ VIOLATION	Identifies the UCMJ violation associated with the outcome record.	LOOKUP	
264	UID NUMBER	Identifies the UID number of the Case record this Adjudicative Outcome Violation record is associated with.	NVARCHAR	10

CUSTOM FIELDS (Adjudicative Outcome Violations table cont'd)

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
265	VIOLATION	Identifies the U.S. Code violation associated with the Adjudicative Outcome record	LOOKUP	
266	VIOLATION TYPE	Identifies the violation type (i.e., USC, USCMJ, CFR, or Other).	LOOKUP	
10	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 37: ADJUDICATIVE OUTCOMES

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
ADJUDICATIVE ACTION	Captures information about adjudicative outcomes (i.e., criminal convictions, acquittals, dismissals; civil judgments or settlements, or administrative outcomes) relative to the parent Adjudicative Action record.	19

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
267	ACTION DATE	Identifies the action date recorded on the parent adjudicative action record	DATE/TIME	
268	ADJUDICATIVE ACTION	Identifies the parent adjudicative action record	LOOKUP	
269	ADJUDICATIVE ACTION TYPE	Identifies the adjudicative action type (e.g., Federal indictment, information, civil complaint, administrative charge, etc.).	LOOKUP	
270	ADJUDICATIVE OUTCOME TYPE	Identifies the adjudicative outcome type (e.g., conviction, acquittal, dismissal, civil settlement, administrative charge, etc.)	LOOKUP	
271	ADJUDICATIVE REFERRAL	Identifies the parent adjudicative referral record to which this record is associated	LOOKUP	
272	ADJUDICATIVE REFERRAL TYPE	Identifies the referral type (i.e., criminal, civil, or administrative).	LOOKUP	
273	CASE	Identifies the case record the action record is associated with.	LOOKUP	
274	DATE VALIDATED	Identifies the date the Action record was validated.	DATE/TIME	
275	OUTCOME DATE	Identifies the date the adjudicative outcome occurred or was filed with the court.	DATE/TIME	
276	REFERRAL AGENCY	Identifies the referral agency.	LOOKUP	
277	REFERRAL DATE	Identifies the referral date.	DATE/TIME	

CUSTOM FIELDS (Adjudicative Outcomes table cont'd)

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
278	SAR PERIOD REPORTED	Identifies the SAR period during which the action was reported.	NVARCHAR	8
279	SAR REPORTABLE	Indicates whether the action is considered SAR reportable.	BIT	
280	SEALED	Indicates whether the action was filed under seal.	BIT	
281	SUBJECT	Identifies the subject record the action record is associated with.	LOOKUP	
282	UID NUMBER	Identifies the UID number of the Case record the action record is associated with.	NVARCHAR	10
283	UNSEALING AUTHORITY	Identifies the unsealing authority (i.e., the person or entity that authorized the unsealing of the court record) relative to the action.	NVARCHAR	100
284	VALIDATED BY	Identifies the name of the person who validated the action.	LOOKUP	
285	VALIDATION STATUS	Identifies the current validation status (i.e., pending validation, submitted for validation, or validated).	LOOKUP	
19	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 38: ADJUDICATIVE REFERRALS

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
CASE SUBJECT	Captures information about adjudicative referrals (i.e., referrals made for criminal, civil, or administrative action) relative to the parent case subject record.	13

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
286	ACCEPT/DECLINE	Yes/No. Identifies whether or not the referral was accepted by the referral agency.	PICKLIST	
287	ADJUDICATIVE REFERRAL TYPE	Identifies the referral type (i.e., criminal, civil, or administrative).	LOOKUP	
288	AGENCY	Identifies the name of the agency to which the referral was made.	LOOKUP	
289	CASE	Identifies the Case record the referral is associated with.	LOOKUP	

CUSTOM FIELDS (Adjudicative Referrals Table, cont'd)

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
290	DECLINE/ACCEPT DATE	Identifies the date the referral was accepted or declined by the referral agency.	DATE/TIME	
291	DECLINE REASON	Identifies the reason the referral was declined.	LOOKUP	
292	OGE REPORTABLE	Yes/No. Identifies whether the referral is reportable to the Office of Government Ethics (i.e., conflict of interest violations).	PICKLIST	
293	PROSECUTORS INFO	OPTIONAL. Captures information about the prosecutor (e.g., name, office, phone, etc.).	NVARCHAR	2,000
294	REFERRAL DATE	Identifies the date the referral was made to the referral agency.	DATE/TIME	
295	REFERRAL LEVEL	Identifies the referral level (e.g., Federal, military, state, foreign, etc.).	LOOKUP	
296	REFERRED FOR S7D	Indicates whether the referral was for suspension and/or debarment of a contractor from Federal contracting.	BIT	
297	SUBJECT	Identifies the parent subject record the referral record is related to.	LOOKUP	
298	UID NUMBER	Identifies the UID number of the Case record the adjudicative referral record is associated with.	NVARCHAR	10
13	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 39: ADJUDICATIVE SENTENCINGS

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
ADJUDICATIVE OUTCOME	Captures information about adjudicative sentencing actions (i.e., criminal, civil, or administrative sanctions) relative to the parent adjudicative outcome record.	25

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
299	ACTION DATE	Identifies the action date recorded on the parent adjudicative action record.	DATE/TIME	
300	ADJUDICATIVE ACTION	Identifies the parent adjudicative action record.	LOOKUP	

CUSTOM FIELDS (Adjudicative Sentencings table cont'd)

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
301	ADJUDICATIVE ACTION TYPE	Identifies the adjudicative action type (e.g., Federal indictment, information, civil complaint, administrative charge, etc.).	LOOKUP	
302	ADJUDICATIVE OUTCOME	Identifies the parent adjudicative outcome record this record is associated with.	LOOKUP	
303	ADJUDICATIVE OUTCOME TYPE	Identifies the adjudicative outcome type (e.g., conviction, acquittal, dismissal, civil settlement, administrative charge, etc.).	LOOKUP	
304	ADJUDICATIVE REFERRAL	Identifies the parent Adjudicative Referral record to which this record is associated	LOOKUP	
305	ADJUDICATIVE REFERRAL TYPE	Identifies the referral type (i.e., criminal, civil, or administrative).	LOOKUP	
306	CASE	Identifies the case record the action record is associated with.	LOOKUP	
307	DATE VALIDATED	Identifies the date the Action record was validated.	DATE/TIME	
308	OUTCOME DATE	Identifies the date the adjudicative outcome occurred or was filed with the court.	DATE/TIME	
309	QUANTITY	Identifies the quantity of the sentencing action (e.g., "36" for 36 months confinement, "1" for 1 suspension or debarment, "10,000" for \$10,000 fine, etc.).	INT	
310	RECEIVING ENTITY	Identifies the agency that received restitution ordered.	LOOKUP	
311	REFERRAL AGENCY	Identifies the referral agency.	LOOKUP	
312	REFERRAL DATE	Identifies the referral date.	DATE/TIME	
313	SAR PERIOD REPORTED	Identifies the SAR period during which the action was reported.	NVARCHAR	8
314	SEALED	Indicates whether the action was filed under seal.	BIT	
315	SENTENCING ACTION	Identifies the sentencing action (e.g., confinement, probation, fine, restitution, etc.)	LOOKUP	
316	SENTENCING DATE	The date the sentencing action was imposed or filed with the court.	DATE/TIME	
317	SAR REPORTABLE	Indicates whether the action is considered SAR reportable.	BIT	

CUSTOM FIELDS (Adjudicative Sentencings table cont'd)

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
318	SUBJECT	Identifies the subject record the action record is associated with.	LOOKUP	
319	UID NUMBER	Identifies the UID number of the case record the action record is associated with.	NVARCHAR	10
320	UNIT	Identifies the unit of measure appropriate for the Sentencing Action selected (e.g., "Each", "Months", "Dollars", etc.)	LOOKUP	
321	UNSEALING AUTHORITY	Identifies the unsealing authority (i.e., the person or entity that authorized the unsealing of the court record) relative to the action.	NVARCHAR	100
322	VALIDATED BY	Identifies the name of the person who validated the action.	LOOKUP	
323	VALIDATION STATUS	Identifies the current validation status (i.e., pending validation, submitted for validation, or validated).	LOOKUP	
25	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 40: ARREST ELEMENTS

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
CASE SUBJECT	Captures information about arrests relative to the parent case subject record.	14

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
324	ARREST CODE	Identifies who made the arrest (e.g., "DCIS agents present and made the arrest," "DCIS agents present but other agency personnel made the arrest," "DCIS agents not present during the arrest," etc.).	LOOKUP	
325	ARREST DATE	Identifies the date the arrest was made.	DATE/TIME	
326	ARREST TYPE	Identifies whether the arrest was made with a warrant.	LOOKUP	
327	ARRESTEE RESIDENCE	Identifies whether the arrestee resides where the crime was committed.	LOOKUP	
328	CASE	Identifies the case record the arrest record is associated with.	LOOKUP	

CUSTOM FIELDS (Arrest Elements table cont'd)

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
329	DATE VALIDATED	Identifies the date the arrest elements record was validated.	DATE/TIME	
330	SAR PERIOD REPORTED	Identifies the SAR period during which the arrest element was reported.	NVARCHAR	8
331	SAR REPORTABLE	Indicates whether the arrest element record is SAR reportable.	BIT	
332	SEALED	Indicates whether or not the arrest element record pertains to an arrest that is currently under seal.	BIT	
333	SUBJECT	Identifies the parent subject record the arrest element record is associated with.	LOOKUP	
334	UID NUMBER	Identifies the UID number of the parent Case record.	NVARCHAR	10
335	UNSEALING AUTHORITY	Identifies the entity that authorized unsealing of the arrest record.	NVARCHAR	100
336	VALIDATED BY	Identifies the person who validated the arrest element record.	LOOKUP	
337	VALIDATION STATUS	Identifies the current validation status (i.e., pending validation, submitted for validation, or validated).	LOOKUP	
14	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 41: CREDIT AGENTS

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
(SEVERAL)	Captures information about agents credited with certain investigative results.	9

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
338	ADJUDICATIVE ACTION	Identifies the adjudicative action record associated with this credit agent record.	LOOKUP	
339	ADJUDICATIVE OUTCOME	Identifies the adjudicative outcome record associated with this credit agent record.	LOOKUP	
340	ADJUDICATIVE REFERRAL	Identifies the adjudicative referral record associated with this credit agent record.	LOOKUP	

CUSTOM FIELDS (Credit Agents table cont'd)

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
341	ADJUDICATIVE SENTENCING	Identifies the adjudicative sentencing record associated with this credit agent record.	LOOKUP	
342	AGENT	Identifies the Agent record associated with this Credit Agent record	LOOKUP	
343	ARREST ELEMENT	Identifies the arrest element record associated with this credit agent record.	LOOKUP	
344	CASE INVESTIGATIVE TECHNIQUE	Identifies the case investigative technique record associated with this credit agent record.	LOOKUP	
345	DISRUPT AND DISMANTLE	Identifies the disrupt and dismantle record associated with this credit agent record.	LOOKUP	
346	RECOVERED GOVERNMENT PROPERTY	Identifies the recovered government property record associated with this credit agent record.	LOOKUP	
9	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 42: CREDIT OFFICES

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
(SEVERAL)	Captures information about offices credited with certain investigative results.	9

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
347	ADJUDICATIVE ACTION	Identifies the adjudicative action record associated with this credit office record.	LOOKUP	
348	ADJUDICATIVE OUTCOME	Identifies the adjudicative outcome record associated with this credit office record.	LOOKUP	
349	ADJUDICATIVE REFERRAL	Identifies the adjudicative referral record associated with this credit office record.	LOOKUP	
350	ADJUDICATIVE SENTENCING	Identifies the adjudicative sentencing record associated with this credit office record.	LOOKUP	
351	AGENT	Identifies the agent record associated with this credit office record.	LOOKUP	

CUSTOM FIELDS (Credit Offices table cont'd)

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
352	ARREST ELEMENT	Identifies the arrest element record associated with this credit office record.	LOOKUP	
353	CASE INVESTIGATIVE TECHNIQUE	Identifies the case investigative technique record associated with this credit office record.	LOOKUP	
354	DISRUPT AND DISMANTLE	Identifies the disrupt and dismantle record associated with this credit office record.	LOOKUP	
355	RECOVERED GOVERNMENT PROPERTY	Identifies the recovered government property record associated with this credit office record.	LOOKUP	
9	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 43: DISRUPT AND DISMANTLE

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
CASE	Captures information about criminal enterprises that have been disrupted or dismantled relative to the parent case record.	9

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
356	CASE	Identifies the case record this record is associated with.	LOOKUP	
357	CRIMINAL ENTERPRISE	Name of the criminal enterprise disrupted or dismantled.	NVARCHAR	100
358	D&D TYPE	Identifies whether the action was a disruption or a dismantlement.	PICKLIST	
359	DATE CLAIMED	Identifies the date the D&D stat was claimed.	DATE/TIME	
360	DATE VALIDATED	Identifies the date the arrest elements record was validated.		
361	DATE VALIDATED	Identifies the date the arrest elements record was validated.	DATE/TIME	
362	SUMMARY NARRATIVE	Identifies summary information about the D&D action taken.	NTEXT	2,000
363	VALIDATED BY	Identifies the person who validated the arrest element record.		

CUSTOM FIELDS (Disrupt and Dismantle table cont'd.)

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
364	VALIDATION STATUS	Identifies the current validation status (i.e., pending validation, submitted for validation, or validated).		
9	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 44: RECOVERED GOVERNMENT PROPERTY

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
CASE SUBJECT	Captures information about recovered Government property relative to the parent Case Subject record.	13

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
365	CASE	Identifies the case record this record is associated with.	LOOKUP	
366	DATE VALIDATED	Identifies the date the arrest elements record was validated.	DATE/TIME	
367	DESCRIPTION	Identifies the description of the items recovered.	NVARCHAR	100
368	PERIOD REPORTED	Identifies the SAR period during which the arrest element was reported.	NVARCHAR	100
369	QUANTITY	Identifies the quantity of the items recovered.	INT	
370	RECOVERY DATE	Identifies the date the items were recovered.	DATE/TIME	
371	SAR REPORTABLE	Indicates whether the arrest elements record is SAR reportable.	BIT	
372	SUBJECT	Identifies the parent subject record with which the arrest element record is associated.	LOOKUP	
373	TOTAL VALUE	Identifies the total value of the items recovered (i.e., Quantity x Unit Value)	MONEY	
374	UID NUMBER	Identifies the UID number of the parent case record.	NVARCHAR	10
375	UNIT VALUE	Identifies the monetary value of each unit of items recovered	MONEY	
376	VALIDATED BY	Identifies the person who validated the arrest element record.	LOOKUP	

CUSTOM FIELDS (Recovered Government Property table cont'd)

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
377	VALIDATION STATUS	Identifies the current validation status (i.e., pending validation, submitted for validation, or validated).	LOOKUP	
13	TOTAL NUMBER OF CUSTOM FIELDS			

TABLE 45: VIOLATIONS CHARGE:

PARENT TABLE NAME	DESCRIPTION	CUSTOM FIELDS
ADJUDICATIVE ACTIONS	Captures information about violations associated with the parent adjudicative action record.	7

CUSTOM FIELDS:

NO.	FIELD NAME	DESCRIPTION	TYPE	SIZE
378	ADJUDCIATIVE ACTION	Identifies the parent adjudicative action record.	LOOKUP	
379	CFR VIOLATION	Identifies the CFR violation associated with the parent Adjudicative Action record.	LOOKUP	
380	COUNTS	Identifies the number of counts.	INT	
381	OTHER VIOLATIONS	Identifies other violations (i.e., not USC, USCMJ, or CFR violations).	NTEXT	2,000
382	UCMJ VIOLATION	Identifies the UCMJ violation associated with the Adjudicative Action record.	LOOKUP	
383	VIOLATION	Identifies the U.S. Code violation associated with the Adjudicative Action record.	LOOKUP	
384	VIOLATION TYPE	Identifies the violation type (i.e., U.S. Code, USCMJ, CFR, or other).	LOOKUP	
7	TOTAL NUMBER OF CUSTOM FIELDS			

ATTACHMENT C

DEFINITIONS OF CRIMS-RELATED TERMS

Briefing Category. The type of briefing conducted. For example, a mission briefing is one that provides information about DCIS mission areas, including fraud awareness training, to non-DCIS personnel in a formal presentation. Briefing categories available in CRIMS are:

- **Mission Briefing.** Mission briefings involve a general description of DCIS mission areas to individuals employed by entities external to DCIS. A mission briefing may also include fraud awareness training.
- **Mission Briefing (Recovery Act).** A mission briefing that involves training associated with DCIS oversight responsibilities under the American Reinvestment and Recovery Act (ARRA) should be categorized as “Mission Briefing (Recovery Act).”
- **Outreach (Recovery Act).** General “outreach” activities for the purpose of identifying points of contact in external entities relative to the ARRA should be categorized as “Outreach (Recovery Act).”

Case. An investigation, project, briefing, or other matter pertaining to the mission and/or operations of the Defense Criminal Investigative Service. See below for the definition of various case types.

Case Category. Identifies the nature of the allegations involved in a particular case.

Case Control Number (CCN). Consists of two elements: the unique identification (UID) number and the case office code (i.e., the 4-digit identifier for each office, such as “40DY”, “60DC”, etc.)). The CCN is generated based on CRIMS data and is placed on investigative reports to fully identify the case the report relates to.

Case Development Package (CDP). A CDP is created the instant a new case record is initiated in CRIMS. The CDP is a precursor to a new case in CRIMS. A case record that has not yet been approved by a case manager for initiation is considered a CDP.

Case Record. A collection of structured and unstructured data that pertains to a particular matter. For example, the case title, case type, case category, etc., are all structured data elements that are a part of a CRIMS case record. Additionally, case documents stored in the VCF contain unstructured data elements (i.e., data that are not contained in specific tables or fields within a database) that also are a part of the CRIMS case record.

Case Type. The kind of case being tracked in CRIMS.

Co-Case Agent. A DCIS employee who has been assigned to actively work on a particular case. Co-case agents are equally involved in the case as the Lead Agent.

Cost Adjustment. A downward adjustment to the total contract price as a result of DCIS investigative efforts, measured in dollars. A copy of the contract modification must be included as support for the SIR Form 1.

Cost Avoidance. “An action taken in the immediate time frame that will decrease costs in the future.” (Source: Glossary of Defense Acquisition Acronyms and Terms (<https://dap.dau.mil/glossary/pages/1674.aspx>)).

Department of Defense (DoD) Nexus. The connection between DoD and the allegations involved in a specified investigation.

Originating Agency. The source of initial allegations or subsequent information on which the initiation or continuation of an investigation is based.

Personally Identifiable Information (PII). Information about an individual that identifies, links, relates, or is unique to, or describes him/her or that can be used to distinguish or trace an individual’s identity, such as SSN; age; date and place of birth; mother’s maiden name; military rank; civilian grade; marital status; race; salary; home or office phone numbers; or other demographic, biometric, personal, medical, and financial information.

Proceeds. Monies received or acquired by a Federal law enforcement agency (i.e., Homeland Security Investigations; Federal Bureau of Investigation) that has statutory authority to receive such monies during a joint authorized undercover operation. Proceeds are used to offset necessary and reasonable expenses (a determination made by the joint agency) incurred in an authorized undercover operation.

Subject. Individuals, businesses, or other organizations associated with cases in CRIMS. Subjects include “suspects,” “witnesses,” “victims,” and “targets.” See Subject Classification for a definition of each.

Subject Classification. The relationship between the subject and the case. The following subject classifications are currently available in CRIMS:

- **Suspect:** An individual, business, or other organization for which sufficient evidence exists to “title and index” it relative to a specific case.
- **Witness:** An individual, business, or other organization that has provided information about the alleged wrongdoing that is the subject of the investigation.
- **Victim:** An individual, business, or other organization that “has suffered direct physical, emotional, or pecuniary harm as a result of the commission of a crime” (42 U.S.C. 10607(e)(2)).

- **Target:** Could also be considered a “Person of Interest.” An individual, business, or other organization that is believed to be involved in some wrongdoing, but for which credible evidence has not yet been developed to justify titling and indexing the person or entity as a “suspect” relative to a specific case. NOTE: this subject classification does NOT refer to a suspect who has been formally named the target of a grand jury investigation.

Subject Type. An individual, a business, or a Government, financial, or religious organization (required by DoD Directive 7730.47).

Unique Identification Number (UID). The system-generated 10-digit identifier automatically assigned by CRIMS to the selected case record when it is created. The first four digits indicate the fiscal year assigned. The next six digits indicate a sequential number assignment within CRIMS relative to the specified fiscal year, beginning with 000001 and continuing through 999999. Once assigned to an investigative effort, a UID cannot be changed.

ATTACHMENT D

CURRENT ADJUDICATIVE TYPES

This attachment lists the current adjudicative Action, outcome, and sentencing types reported in CRIMS.

Adjudicative Action Types:

Action Type	Referral Type
FEDERAL INDICTMENT	CRIMINAL
FEDERAL INFORMATION	CRIMINAL
FEDERAL PRE-TRIAL DIVERSION	CRIMINAL
FOREIGN GOVERNMENT CHARGE (ALL TYPES)	CRIMINAL
NON-PROSECUTIVE AGREEMENT (ACTION)	CRIMINAL
OTHER CRIMINAL CHARGE	CRIMINAL
RULE 20 – TRANSFER TO/FROM ANOTHER JUDICIAL DISTRICT	CRIMINAL
STATE/LOCAL CHARGE (ALL TYPES)	CRIMINAL
UCMJ PREFERRAL OF CHARGES (ARTICLE 32 COURTS-MARTIAL)	CRIMINAL
FEDERAL CIVIL COMPLAINT	CIVIL
FEDERAL CIVIL SETTLEMENT AGREEMENT	CIVIL
FEDERAL MOTION TO JOIN QUI TAM COMPLAINT	CIVIL
STATE/LOCAL CIVIL ACTION	CIVIL
ADMINISTRATIVE CHARGE	ADMINISTRATIVE
UCMJ NON-JUDICIAL PUNISHMENT (ARTICLE 15 (ACTION)	ADMINISTRATIVE

Adjudicative Outcome Types:

Outcome Type	Referral Type
ACQUITTAL	CRIMINAL
CONVICTED OF A LESSER OFFENSE	CRIMINAL
CONVICTION	CRIMINAL
DISMISSAL (CRIMINAL)	CRIMINAL
NON PROSECUTIVE AGREEMENT (OUTCOME)	CRIMINAL
PRE TRIAL DIVERSION	CRIMINAL
RULE 20 CONSOLIDATION	CRIMINAL
CIVIL CONVICTION	CIVIL
CIVIL SETTLEMENT	CIVIL
DISMISSAL (CIVIL)	CIVIL
ADMINISTRATIVE NO ACTION	ADMINISTRATIVE
ADMINISTRATIVE OUTCOME	ADMINISTRATIVE
UCMJ NON-JUDICIAL PUNISHMENT (ARTICLE 15) (OUTCOME)	ADMINISTRATIVE

Adjudicative Sentencing Types:

Sentencing Action	Unit	Referral Type
CAPITAL PUNISHMENT	Each	CRIMINAL
CONFINEMENT	Months	CRIMINAL
CONFINEMENT – LIFE SENTENCE	Each	CRIMINAL
CONFINEMENT SUSPENDED	Months	CRIMINAL
DEPORTATION (Criminal)	Each	CRIMINAL
FINE (Criminal)	Dollars	CRIMINAL
FINE SUSPENDED (Criminal)	Dollars	CRIMINAL
MILITARY DISCHARGE (CRIM)	Each	CRIMINAL
MILITARY GRADE REDUCTION	Each	CRIMINAL
NO SENTENCING ACTION (CRIMINAL)	Each	CRIMINAL
NON-U.S. GOV\$ RESTITUTION (Criminal)	Dollars	CRIMINAL
OTHER MONETARY (Criminal)	Dollars	CRIMINAL
OTHER NON-MONETARY (Criminal)	Each	CRIMINAL
PENALTY ASSESSMENT (Criminal)	Dollars	CRIMINAL
PROBATION	Months	CRIMINAL
PROBATION – LIFETIME	Each	CRIMINAL
PUBLIC SERVICE	Hours	CRIMINAL
RESTITUTION U.S. GOV\$ (Criminal)	Dollars	CRIMINAL
TRICARE - RESTITUTION U.S. GOV\$ (CRIMINAL)	Dollars	CRIMINAL
DEPORTATION (Civil)	Each	CIVIL
FINE (Civil)	Dollars	CIVIL
FINE SUSPENDED (Civil)	Dollars	CIVIL
NO COST REPAIR/REPLACEMENT OF GOODS OR SERVICES (Civil)	Dollars	CIVIL
NO SENTENCING ACTION (CIVIL)	Each	CIVIL
NON-U.S. GOV\$ RESTITUTION (Civil)	Dollars	CIVIL
OTHER NON-MONETARY (Civil)	Each	CIVIL
PENALTY ASSESSMENT (Civil)	Dollars	CIVIL
RESTITUTION U.S. GOV\$ (Civil)	Dollars	CIVIL
TRICARE - RESTITUTION U.S. GOV\$ (CIVIL)	Dollars	CIVIL
ART 15 - ADMIN DISCHARGE	Each	ADMINISTRATIVE
ART 15 - BAR FM REENLIST	Each	ADMINISTRATIVE
ART 15 - EXTRA MIL DUTY	Each	ADMINISTRATIVE
ART 15 - RESTITUTION	Dollars	ADMINISTRATIVE
ART 15 - RESTRICTION	Each	ADMINISTRATIVE
ART 15 - UCMJ FINE	Dollars	ADMINISTRATIVE
ART 15 - UCMJ FORFEITURE	Dollars	ADMINISTRATIVE
BID REJECTION	Each	ADMINISTRATIVE
CLEARANCE TERMINATION	Each	ADMINISTRATIVE
CONTRACT TERMINATION	Each	ADMINISTRATIVE
COST ADJUSTMENT	Dollars	ADMINISTRATIVE
DEBARMENT FM CONTRACTS	Each	ADMINISTRATIVE
DEMOTION/GRADE REDUCTION	Each	ADMINISTRATIVE
DEPORTATION (Admin)	Each	ADMINISTRATIVE

Sentencing Action	Unit	Referral Type
EXCLUSION	Each	ADMINISTRATIVE
JOB SUSPENSION	Each	ADMINISTRATIVE
JOB TERMINATION	Each	ADMINISTRATIVE
LEAVE WITHOUT PAY	Each	ADMINISTRATIVE
MILITARY DISCHARGE (ADMIN)	Each	ADMINISTRATIVE
NO COST REPAIR/REPLACEMENT OF GOODS OR SERVICES (Admin)	Dollars	ADMINISTRATIVE
NON-U.S. GOV\$ RESTITUTION (Admin)	Dollars	ADMINISTRATIVE
OCCUPATION RECLASSIFY	Each	ADMINISTRATIVE
OTHER MONETARY (Admin)	Dollars	ADMINISTRATIVE
OTHER NON-MONETARY (Admin)	Each	ADMINISTRATIVE
PFCRA ACTION	Dollars	ADMINISTRATIVE
PROCEEDS (Admin)	Dollars	ADMINISTRATIVE
RECOUP PREVIOUS U.S.\$	Dollars	ADMINISTRATIVE
RESTITUTION U.S. GOV\$ (Admin)	Dollars	ADMINISTRATIVE
SUSPENSION FM CONTRACTS	Each	ADMINISTRATIVE
TRICARE - RESTITUTION U.S. GOV\$ (ADMIN)	Dollars	ADMINISTRATIVE
CONTRACTOR DISCLOSURE	Dollars	ADMINISTRATIVE
WRITTEN WARNING/REPRIMAND	Each	ADMINISTRATIVE

ATTACHMENT E

VALIDATION OF INVESTIGATIVE RESULTS

Validation Authority:

- All monetary investigative results, to include entries in Adjudicative Sentencing and Recovered Government Property
 - Valued under \$500,000
 - RAC, ASAC, or SAC
 - Valued \$500,000 or over
 - Internal Operations Directorate analysts
- Non-monetary investigative results, including entries in Adjudicative Actions, Adjudicative Outcomes, Adjudicative Sentencing, and Arrests
 - RAC, ASAC, or SAC

The following table provides guidance concerning the validation requirements for investigative results reported in the Case Reporting and Information Management System (CRIMS).

RESULT TYPE	DATES	SUPPORTING DOCUMENTATION
Adjudicative Referral	Date investigation was presented to prosecutor or other official for action	None required
Adjudicative Action		
• Federal Information	Date the charging document was filed or stamped by the clerk of the court	Charging document filed by the court
• Federal Indictment		
• State/Local Charge		
• Foreign Government Charge		
• Administrative Charge	Same date as the Referral or the Sentencing Action	None required
• UCMJ Non-Judicial Punishment	Decision date on form or memorandum date	Record of Proceedings Under Article 15, UCMJ (DA Form 2627, AF Form 3070 or NAVPERS Form 1070) or Report of Proceedings by Investigating Officer/Board of Officers (DA Form 1574) or Memorandum of Reprimand
• Federal Civil Complaint	Date the document was filed or stamped by the clerk of the court	Court-filed or stamped civil complaint
• State/Local Civil Action		Court-filed or -stamped civil complaint or suit filed in a state or local venue
• Federal Motion to Joint Qui Tam Complaint		Court-filed or -stamped motion filed by the Government to join the <i>qui tam</i>

RESULT TYPE	DATES	SUPPORTING DOCUMENTATION
<ul style="list-style-type: none"> Federal Civil Settlement Agreement 	Date of final signature on the document	Settlement agreement signed by all parties
<ul style="list-style-type: none"> Other Adjudicative Actions 	Date event occurred	Documentation from an official source (court, municipality, military Service etc.) substantiating the event occurred. Contact the Internal Operations Directorate for specific determinations.
Adjudicative Outcome		
<ul style="list-style-type: none"> Conviction 	For convictions based on guilty pleas, use the date the court accepted the plea, which is generally the date the plea was entered. For convictions by jury, use the date the jury found the defendant guilty.	For convictions based on plea accepted by the court, use the docket minutes or any document from the court indicating the judge has accepted the plea. If substantiated documentation indicating acceptance of the plea cannot be obtained, use the date the defendant was sentenced. For verdict of guilty by jury, use the docket minutes or any document from the court stating that the defendant has been found guilty.
<ul style="list-style-type: none"> Civil Settlement 	Date of final signature on the document	Civil settlement agreement signed by all parties
<ul style="list-style-type: none"> Administrative Action Administrative No Action 	Same date as the referral or the sentencing action	No documents required
<ul style="list-style-type: none"> Civil Conviction 	Date of judge's determination of guilt, summary judgment, or of jury verdict	Court-filed or -stamped order, judgment, or verdict form
<ul style="list-style-type: none"> Non-Prosecution Agreement 	Date of final signature on the document	Non-prosecution agreement signed by all parties
<ul style="list-style-type: none"> Federal Pre-Trial Diversion 	Date of final signature on the document	Signed pre-trial diversion agreement
<ul style="list-style-type: none"> Acquittal 	Date of verdict	Court-filed or -stamped verdict form
<ul style="list-style-type: none"> Dismissal 	Court-filed date of order dismissing charges	Court-filed or -stamped order dismissing charges
<ul style="list-style-type: none"> Other Adjudicative Outcomes 	Date event occurred	Documentation from an official source (court, municipality, military Service etc.) substantiating the event occurred. Contact the Internal Operations Directorate for specific determinations.

Adjudicative Sentencing		
<ul style="list-style-type: none"> • Confinement/ Confinement Suspended • Fine (Criminal)/ Fine Suspended (Criminal) • Penalty Assessment (Criminal) • Probation 	Date the sentence was imposed	Judgment (i.e., "J&C") filed by the court, pre-trial diversion agreement, or non-prosecution agreement
<ul style="list-style-type: none"> • Restitution U.S. Gov\$ 	<p>For criminal judgment, the imposition date of the sentence.</p> <p>For a civil settlement, the date of the final signature on the agreement</p> <p>For administrative recoveries, the date of the agreement or the date the funds were obtained</p>	Judgment (J&C) filed by the court; pre-trial diversion agreement or non-prosecution agreement; civil settlement agreement signed by all parties or civil judgment ordering payment; administrative settlement agreement; demand letter signed by suspect or proof of payment in response to a demand letter; or documentation from Article 32 UCMJ or Article 15 nonjudicial punishment documentation from an official source, such as a court, municipality, or Military Service substantiating the event occurred
<ul style="list-style-type: none"> • Non-U.S. Gov\$ Restitution 	<p>For criminal judgment, the imposition date of the sentence.</p> <p>For a civil settlement, the date of the final signature on the agreement</p>	Monies not going to the Federal Government must be reported separately as nongovernment restitution and subtracted separately. This can include the relator's share from a <i>qui tam</i> settlement, state shares of Medicaid recoveries, money going to individuals or companies. The amount can be documented via a victim's list on a judgment, stipulated in a civil settlement agreement, listed on a Civil Fraud Tracking Sheet, or provided from correspondence with the United States Attorney's Office.
<ul style="list-style-type: none"> • TRICARE- Restitution U.S. Gov\$ 	<p>For criminal judgment, the imposition date of the sentence.</p> <p>For a civil settlement, the date of the final signature on the agreement</p>	In health care investigations, any amount being returned to TRICARE or Defense Health Agency must be reported separately as TRICARE restitution. The amount can be substantiated by a Civil Fraud Tracking Sheet, broken out in correspondence from the United States Attorney's Office, listed separately on a judgment, or specified in an administrative agreement.

• Fine (Civil)/ Fine Suspended (Civil)	For a civil settlement, the date of the final signature on the agreement	Civil Settlement Agreement signed by all parties or civil judgment ordering payment
• Suspension	Effective date of suspension or date of notification letter	Notification letter of suspension or proposed debarment or screenshot/print out from System for Award Management website, www.sam.gov
• Debarment	Effective date of debarment or date of notification letter	Notification letter of debarment or screenshot/printout from System for Award Management website, www.sam.gov
• No Cost Repair/Replacement of Goods or Services	Date of settlement agreement, date of contract modification, or date of correspondence from contractor agreeing to replacement/repair	Settlement agreement, contract modification, correspondence for contractor detailing the repair or replacement of goods or services at no cost to the Government
• Military Discharge (Criminal)	Effective date of court martial decision/ memorandum date	Military form or memorandum documenting the results of a court martial
• Military Grade Reduction	Effective date of court martial decision/ Article 15 outcome or memorandum date	Military form or memorandum documenting the results of a court martial Record of Proceedings Under Article 15, UCMJ document (DA Form 2627) or Report of Proceedings by Investigating Officer/Board of Officers (DA Form 1574) or Memorandum of Reprimand
• Article 15 Actions (i.e. Discharge, Restriction, UCMJ Forfeiture, UCMJ Fine, etc.)	Decision date on DoD form or memorandum date	Record of Proceedings Under Article 15, UCMJ document (DA Form 2627) or Report of Proceedings by Investigating Officer/Board of Officers (DA Form 1574) or Memorandum of Reprimand
• Military Discharge (Admin)		
• Cost Adjustment	Date of contract modification	Contract modification
• Contract Termination	Date contract terminated	Termination letter

<ul style="list-style-type: none"> • Proceeds 	Date proceeds were obtained	Report stating funds are proceeds of an undercover operation. Proceeds are monies received or acquired by a Federal law enforcement agency that has statutory authority to receive such monies during a joint undercover operation. DCIS may report in CRIMS the total amount of “proceeds” received by the joint Federal investigative agency after DCIS has initiated a spin-off investigation. “Proceeds” are separate and distinct from “seizures” and must be clearly identified on supporting documentation (Form 1’s, Memorandums for the Record, other agency reports, etc.).
<ul style="list-style-type: none"> • Other Adjudicative Sentencing 	Date event occurred	Documentation from an official source (court, municipality, military Service etc.) substantiating the event occurred. Contact the Internal Operations Directorate for specific determinations.
Arrest	Date arrest occurred	Arrest warrant with return portion filled in (documenting warrant was executed) or Public Access to Court Electronic Records (PACER) entry documenting arrest occurred
Recovered Government Property	Date property recovered	SIR and documentation to substantiate claimed amount such as official Government documents, sales transaction information, appraisals, other third-party documentation, and/or photographs supporting the claimed value given the condition of the items recovered

- Confinement/probation (i.e., supervised release) can be concurrent or consecutive. Consecutive terms may be summed to determine the total time of confinement or probation. Concurrent terms cannot be summed, and only the value of the longest term should be used.
- Home confinement/ house arrest is entered into CRIMS as confinement
- When restitution is to be paid jointly and severally between several co-defendants, the amount should be split among them so as to not overstate the total restitution amount when all of the subjects’ individual restitution amounts are summed in CRIMS.

ATTACHMENT F

CONFIGURATION MANAGEMENT PROCEDURES

PURPOSE:

The purpose of configuration management is to implement a formal and structured change-control system to ensure beneficial changes are implemented while avoiding the consequences of making changes haphazardly. Change control is the process of planning, scheduling, communicating, and executing changes. The goal is to establish clear policies and procedures that promote the successful introduction of change while minimizing negative impact and maximizing resource availability.

The purpose of this document is to provide clear policies and procedures on the change-control process for the CRIMS application.

APPLICABILITY:

The change control process described here pertains to *all* requested changes that affect the functionality or look and feel of the CRIMS application. Some change requests will require minimal review and can be approved by the CRIMS program manager; other change requests require formal review and approval by the Change Control Board (CCB). The procedures in this document apply to all DCIS personnel.

ROLES AND RESPONSIBILITIES:

The following roles and responsibilities apply to the CRIMS change control process:

CCB—The goal of the CCB is to promote a smooth and harmonious enhancement of the CRIMS application over time. This will be accomplished by ensuring a structured process is used to consider proposed changes and incorporate them into specified releases of the CRIMS application. The CCB will review change requests, analyze their possible effects, make decisions, and communicate them to the appropriate parties.

The CCB consists of voting members and advisors. Voting members have the authority to approve or decline any change request the CCB considers. Advisory members provide guidance and make recommendations to voting members but do not have the authority to approve or deny any change request.

Voting Members:

- CCB chair
- CRIMS program manager or designee
- Program Director, Special Projects (04SP), or designee

Advisory Members:

- Subject-matter experts relative to the requested change, as appropriate;
- ISD representatives, as appropriate;
- Representatives from other OIG components, as appropriate (e.g., Comptroller's office).

CCB Responsibilities:

- Review all change requests that require CCB approval. (See change categories section below).
- Perform a cost/benefit analysis to ensure the stated benefit outweighs the cost and/or potentially negative impact that might result.
- Represent the interests of all stakeholders who may be affected by any proposed changes.
- Approve or deny requested changes.
- Document the reasons for each approval or denial of a change request.

CCB Chair—The SAC, Internal Operations, serves as the CCB chair. The CCB chair is not required to participate in all CCB deliberations but may choose to do so. The primary role of the CCB chair is to mediate any differences among the other voting members of the CCB on the approval or disapproval of a change request. The CCB chair will consider all change requests submitted for his or her approval and explain in writing to the other voting members his or her approval or denial of the request. The CCB chair may consult other DCIS senior managers or the heads of OIG components (e.g., ISD Chief, Comptroller, etc.) in making these decisions.

Change Manager—The CRIMS program manager serves as the change manager. The change manager is responsible for:

- receiving and reviewing all change requests for completeness;
- obtaining additional information, as necessary, from the requestor to facilitate proper consideration by the CCB;
- categorizing all change requests according to the categories listed below;

- entering details about proposed changes in the change log;
- providing the CCB members with written change requests and all supporting information necessary for the CCB to properly consider the change request;
- coordinating CCB discussions regarding proposed changes;
- compiling the documented CCB decision to approve or disapprove a change request;
- updating the change log with the CCB decision; and
- communicating the CCB decision to appropriate parties promptly.

CHANGE-REQUEST CATEGORIES:

Although *all* change requests must be submitted in writing and documented in the change log, it would be impractical for the CCB to consider all requests for changes to the CRIMS application. Therefore, the following categories will be applied.

- **Routine**—Involve negligible impact on the scope, schedule, and/or cost related to the development, deployment, or maintenance of CRIMS. Routine change requests *do not* require CCB approval. Examples are adding options to lookup tables or pick lists relative to existing fields.
- **Mandated**—Requests for changes mandated by statute, regulation, or external policy requirements. Mandated change requests *do not* require CCB approval. Examples are adding new data fields and tables to support DIBRS and D-DEx reporting requirements.
- **Optional Enhancement**—Changes proposed by stakeholders to improve the functionality of the CRIMS application to meet an optional preference. Such change requests *do* require CCB approval. Examples are adding a new field to an existing table, adding a new table, creating new relationships between tables, creating a new user role or modifying permissions for an existing role, and creating a new business process workflow or modifying changes to an existing workflow.

CHANGE CONTROL PROCESS:

The change control process is as follows.

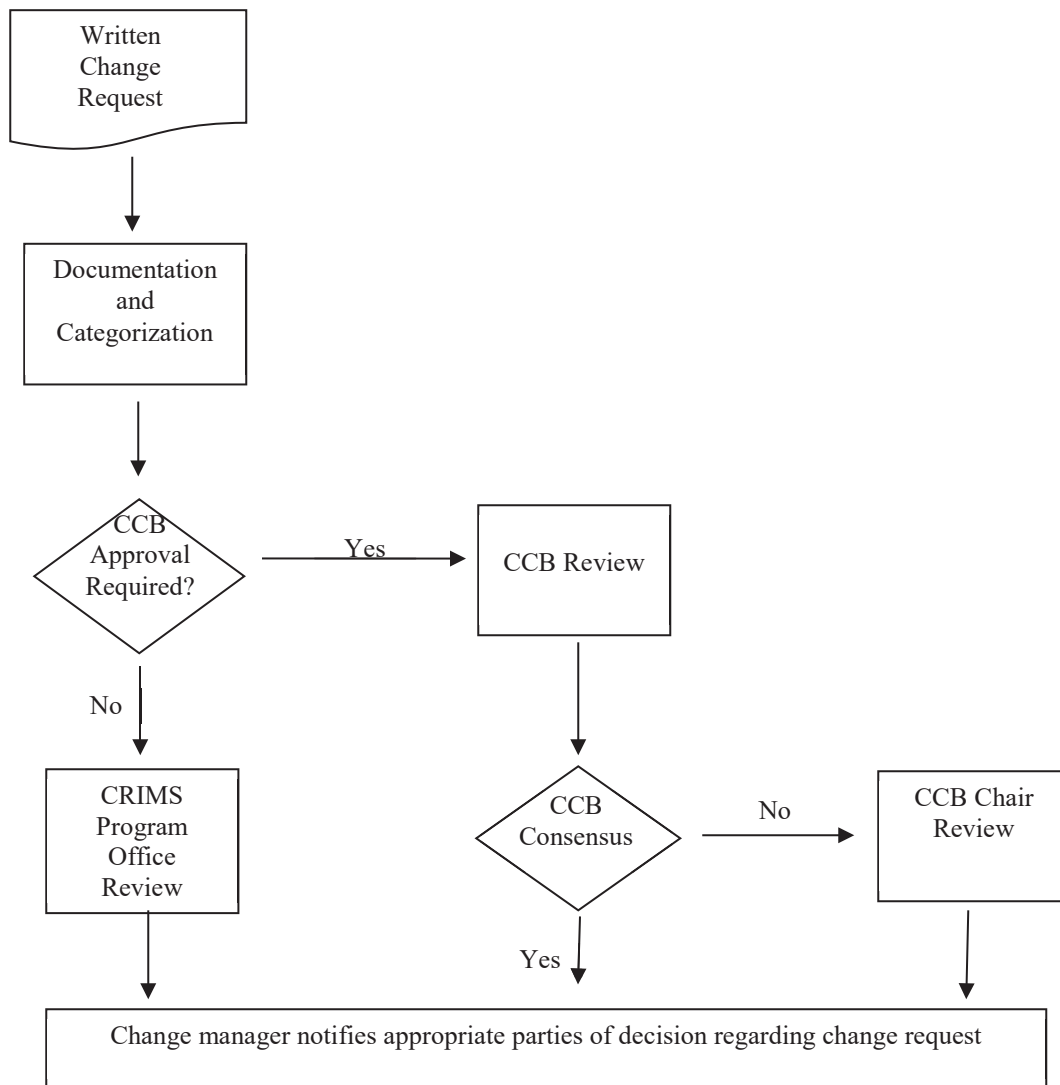
1. A written change request must be submitted to the change manager to initiate the change control process. Change requests may be submitted in any written format (e.g., e-mail), but they must include:

- a. *a detailed* description of the requested change;
 - b. the business case for the requested change (for which *there must be a valid business reason*); and
 - c. known costs or potential negative impact associated with implementation of the requested change.
2. The change manager will document the request, make an entry in the change log, and assign a change category, which will be used to determine if the change request must be reviewed by the CCB. Additionally, the change manager will notify the SACs for Investigative and International Operations of the proposed change. The SACs for Investigative and International Operations will be afforded the opportunity to comment on the proposed change.
3. If the change request does not require CCB review (see change categories above), the change manager will take appropriate steps to approve/disapprove the change, update the change log, and communicate the decision to the appropriate parties.
4. If the change request requires CCB review (see change categories above), the change manager will provide the CCB members with written information about the requested change and coordinate CCB discussions on approval/disapproval of the proposed change.
5. The CCB will review change requests requiring CCB approval, perform cost/benefit analysis regarding the impact of the change, and issue a decision on approval/disapproval of the requested change.
6. If the CCB reaches a consensus regarding the approval/disapproval of the requested change, they will communicate their decision in writing to the change manager. The

change manager will update the change log with the CCB decision and communicate the decision to the appropriate parties.

7. If the CCB cannot reach a consensus on the approval/disapproval of the requested change, the change request will be elevated to the CCB chair, with notification to the SACs for Investigative and International Operations. The CCB chair will review the CCB analysis; consult senior managers, SMEs, and/or other OIG component heads as necessary; and issue a decision . The change manager will update the change log and communicate the decision to appropriate parties.

PROCESS FLOWCHART:





INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

February 11, 2015

MEMORANDUM FOR ALL DCIS SPECIAL AGENTS

SUBJECT: Interim Policy for Special Agents Manual (SAM) Chapter 50, Case Reporting and Information Management System; Regarding Reporting of Confinement and Probation and Rounding of Monetary Amounts

Effective immediately, this interim policy modifies guidance provided in Attachment E of SAM Chapter 50 regarding the reporting of confinement and probation (i.e., supervised release) and the rounding of monetary amounts reported in CRIMS. Attachment E currently states:

“Confinement/probation (i.e., supervised release) can be concurrent or consecutive. Consecutive terms may be summed to determine the total time of confinement or probation. Concurrent terms cannot be summed, and only the value of the longest term should be used.”

This resulted in artificial reductions in the amount of probation reported in CRIMS when the probation runs concurrent with a period of confinement. In order to correct this, the language on Attachment E is modified to read as follows:

“Confinement can be concurrent or consecutive. Consecutive terms may be summed to determine the total time of confinement. Concurrent terms cannot be summed, and only the value of the longest term should be used.”

Periods of home confinement and probation will be counted separately, even if they overlap. For example, if a defendant is ordered to complete 36 months of home confinement and 6 months of probation, and the probation runs concurrent with the period of home confinement, you would report 36 months of confinement and 6 months of probation.

Monetary amounts reported in CRIMS should be rounded to the nearest whole dollar. For amounts below \$0.50, round down to the lower whole dollar amount. For amounts equal to or above \$0.50, round up to the next whole dollar amount.

This interim policy is in effect until it is rescinded or incorporated into the next revision of SAM Chapter 50. Any questions related to this policy should be directed to (b)(6), (b)(7)(C) Program Manager, Case Reporting and Information Management System at (b)(6), (b)(7)(C) @dodig.mil.

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

Deputy Assistant Inspector General
for Investigations



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

February 27, 2015

MEMORANDUM FOR ALL DCIS SPECIAL AGENTS

SUBJECT: Interim Policy for Special Agents Manual (SAM) Chapter 50, Case Reporting and Information Management System; Regarding Top 100 Defense Contractor Tracking

CRIMS has a mechanism for case agents to flag investigations opened involving a Top 100 Defense Contractor. However, the use of this flag was inconsistent and the designation did not support any internal or stakeholder reporting requirements.

Effective immediately, paragraph 50.8.e, requiring use of this flag, is rescinded. There is no prohibition against including the "Top 100" designation in the Case Initiation Report or Case Summary, as appropriate. Agents can identify these companies by reviewing the Top 100 Defense Contractors list maintained in the Special Agent Toolbox under the Resources tab.

This interim policy is in effect until rescinded or incorporated into the next revision of SAM Chapter 50. Any questions related to this policy should be directed to (b)(6), (b)(7)(C) Program Manager, Case Reporting and Information Management System at (b)(6), (b)(7)(C)@dodig.mil.

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

Deputy Assistant Inspector General
for Investigations



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

July 30, 2015

MEMORANDUM FOR ALL DCIS SPECIAL AGENTS

SUBJECT: Interim Policy for Special Agents Manual (SAM) Chapter 50, Case Reporting and Information Management System; Regarding Digital Signatures.

Effective immediately, paragraph 50.7.h., Digital Signatures, requiring a digital signature on all DCIS-issued investigative reports uploaded to the Virtual Case File, is rescinded.

Removing this paragraph removes the requirement for only digital signatures to be used on documents uploaded to CRIMS. Any questions regarding the placement or number of signatures required on investigative reports are addressed in SAM Chapter 28, Investigative Reports.

This interim policy is in effect until it is rescinded or incorporated into the next revision of SAM Chapter 50. Any questions related to this policy should be directed to (b)(6), (b)(7)(C) Program Director, CRIMS, Analysis & Communications at (703) 604-5, (b)(7) or (b)(6), (b)(7)(C) @dodig.mil.

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

Deputy Assistant Inspector General
for Investigations



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

February 25, 2016

MEMORANDUM FOR ALL DCIS SPECIAL AGENTS

SUBJECT: Interim Policy for Special Agents Manual (SAM) Chapter 50, "Case Reporting and Information Management System (CRIMS)," regarding Case Manager Reviews of the Case Development Packages (CDP)

Effective immediately, this interim policy changes the location of the case manager notes regarding CDPs over 90 days old. The following language is hereby rescinded from SAM Chapter 50, paragraph 50.6.a.:

CDPs are the initial entries that lead to an open investigation/information report. They are intended to help agents collect information immediately before beginning an investigation/information report. CDPs may not remain open longer than 90 days without a note (made via the Initiation tab on the CRIMS Case form) indicating the CDP has been reviewed by the case manager. After the first 90 days, the CDP record must be reviewed every 30 days; this review should be noted on the Initiation tab until the case has been approved or the CDP has been disapproved. Consult SAM Chapter 28 for policy guidance on when a CDP should be converted to an open investigation/information report.

Effective immediately, this interim policy updates SAM Chapter 50, paragraph 50.6.a. to read as follows:

CDPs are the initial entries that lead to an open investigation/information report. They are intended to help agents collect information immediately before beginning an investigation/information report. CDPs may not remain open longer than 90 days without a note in the Comment field of the RAC Review entity (left navigation pane) indicating the CDP has been reviewed by the case manager. After the first 90 days, the CDP record must be reviewed every 30 days until the case has been approved or the CDP has been disapproved. This 30-day review should also be captured in the Comment field of the RAC Review. Consult SAM Chapter 28 for policy guidance on when a CDP should be converted to an open investigation/information report.

This policy is in effect until it is rescinded or incorporated into the next revision of SAM Chapter 50. Any questions related to this policy should be directed to me at (703) 604-6, (b)(7)

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

Deputy Assistant Inspector General
for Investigation

CHAPTER 51 (Administration)

CRITICAL INCIDENT MANAGEMENT

<u>Contents</u>	<u>Section</u>
General	51.1.
Policy	51.2.
Definitions	51.3.
Critical Incident Procedures for	
Field Supervisors	51.4.
DCIS Headquarters Responsibilities	51.5.
Field Management Responsibilities	51.6.
Post-Incident Procedures	51.7.
Management Followup	51.8.
Peer Support Service	51.9.
Undercover Operations	51.10.

51.1. General

51.1.a. This chapter establishes the Defense Criminal Investigative Service (DCIS) policy, procedures, and guidelines regarding DCIS personnel involved in a critical incident. The guidelines may be uniformly applied following any incident that has resulted in death or serious bodily injury, or any critical incident. These guidelines are in effect to reduce the chances that DCIS personnel will develop or suffer from post-traumatic stress disorder (PTSD) resulting from a critical incident.

51.1.b. This policy applies to all DCIS personnel assigned to field elements and DCIS Headquarters (HQ) regardless of physical location or assignment.

51.1.c. DCIS will have one or more personnel specially trained in critical incident stress management (CISM) techniques. One individual will be designated as the DCIS Peer Support Program Coordinator and will coordinate the CISM program.

51.2. Policy

51.2.a. A shooting incident is possibly the most severe occupational stress that a special agent is likely to experience during his or her career. The duties of a special agent can expose him or her to mentally disturbing and highly stressful situations that cannot be resolved through normal stress coping mechanisms. Unless adequately treated, these situations can create disabling emotional and physical problems. It has been found that agent-involved incidents resulting in death or serious bodily injury may precipitate such stress disorders. It is the responsibility of DCIS to provide our personnel with information on stress disorders and to guide

and assist in its deterrence. It is DCIS policy to take immediate action after such incidents to safeguard the continued good physical and mental health of all involved DCIS personnel. These requirements do not take the place of the reporting requirements contained in the DCIS Special Agents Manual (SAM), Chapter 38, "Use of Force," paragraph 38.2.o., relating to the discharge of a firearm, nor SAM Chapter 36, "Motor Vehicles," paragraph 36.22., relating to the investigation of a motor vehicle accident.

51.2.b. The Special Agent in Charge or designated representative is required to contact the agency-designated Peer Support Program Coordinator as soon as practical but within 12 hours of an agent-involved incident that has resulted in a death or severe bodily injury. All DCIS personnel directly involved in the shooting incident shall be required to meet with either a Peer Support specialist or a health care professional. DCIS managers are encouraged to contact the Peer Support Program Coordinator for assistance regarding any other type of critical incident.

51.2.c. DCIS managers should strongly suggest and encourage individuals who experience a critical incident where contact with peer support is not mandatory, to contact the DCIS Peer Support Program Coordinator. Contact should be initiated as soon as possible after the incident, generally within 24-48 hours.

51.2.d. All DCIS personnel may directly contact the agency-designated Peer Support Program Coordinator to request assistance after experiencing a critical incident.

51.3. Definitions. The following definitions apply throughout this chapter.

51.3.a. **Post-Traumatic Stress Disorder.** An anxiety disorder that can result from exposure to short-term severe stress, or the long-term buildup of repetitive and prolonged milder stress. It may result from exposure to a critical incident.

51.3.b. **Agent-Involved Shooting Incident.** A line-of-duty incident where a shooting causes death or bodily injury to the special agent or other person.

51.3.c. **Critical Incident.** Any situation faced by agency personnel that has a stressful impact sufficient enough to overwhelm the usually effective coping skills of either an individual or a group. The incident may have the potential to interfere with the ability to function either at the scene or later. Exposure to any critical incident may serve as a starting point for PTSD.

51.3.d. **Defusing.** The word defusing means to render something harmless before it can do damage. A defusing is a small group process that is instituted after any critical incident powerful enough to overwhelm the coping mechanisms. It may also serve as an early identification for individuals who may require professional mental health followup.

51.3.e. **Critical Incident Stress Debriefing.** A group meeting and discussion about a critical incident with a Peer Supporter(s). The meeting is designed to mitigate the impact of a critical incident and to assist the personnel impacted in recovering as quickly as possible from the stress associated with the incident.

51.3.f. **Peer Support Specialist.** A special agent who is trained in CISM, PTSD, and the techniques of intervention. The training must be received from a recognized/accredited institution and/or mental health professional.

51.3.g. **Peer Support Program Coordinator.** A special agent who coordinates/manages the DCIS CISM program. This individual will meet the same requirements as the Peer Support specialist.

51.4. Critical Incident Procedures for Field Supervisors

(b)(7)(E)

ATTACHMENT A

SAMPLE PRESS RELEASE

PRESS RELEASE

DEFENSE CRIMINAL INVESTIGATIVE SERVICE
OFFICE OF THE INSPECTOR GENERAL
DEPARTMENT OF DEFENSE

On [date] at [time] , employee(s) of the Defense Criminal Investigative Service, Office of the Inspector General of the Department of Defense, was (were) involved in a critical incident. The incident is currently being investigated by the [name of police department and/or the FBI] , therefore, it would be premature to offer any additional information at this time. As soon as additional details are obtained, they will be released by [name] , Deputy Inspector General for Investigations, in Washington, DC, who can be reached at (703) 604-8600.

CHAPTER 54 (Administration)

LAW ENFORCEMENT AVAILABILITY PAY

<u>Contents</u>	<u>Section</u>
Introduction	54.1.
Definitions	54.2.
Eligibility	54.3.
General Rules	54.4.
Reporting Requirements	54.5.
Biweekly Activity Report, DCIS Form 54	54.6.
Workhour Tracking System (WTS)	54.7.

54.1. Introduction. This chapter provides standardized policy, guidelines, and procedures for the payment of availability pay for unscheduled work performed by criminal investigators of the Defense Criminal Investigative Service (DCIS), Office of the Deputy Inspector General for Investigations (ODIG-INV), Office of the Inspector General (OIG) of the Department of Defense (DoD). Law Enforcement Availability Pay (LEAP) for criminal investigators is covered by title 5, United States Code (USC), section 5545a and Public Law 103-329, as amended.

54.2. Definitions

54.2.a. Law Enforcement Availability Pay. LEAP is the 25 percent premium pay granted in the Law Enforcement Availability Pay Act of 1994. It is paid to ensure the availability of criminal investigators for unscheduled duty in excess of a 40-hour workweek based on the needs of the ODIG-INV. LEAP will be considered as part of basic pay for the computation of advances in pay, severance pay, worker's compensation, Thrift Savings Plan, retirement benefits, lump sum annual leave, and life insurance.

54.2.b. Available. Available means that a criminal investigator shall be either performing official duties during unscheduled duty hours or considered generally and reasonably accessible to perform official duties during unscheduled duty hours based on the needs of the ODIG-INV. The criminal investigator is generally responsible for recognizing, without supervision, circumstances that require the criminal investigator to be on duty or available for unscheduled duty based on the needs of the agency. However, the supervisor may place a criminal investigator in availability status by directing the criminal investigator to be available to respond to specific ODIG-INV needs during designated periods. LEAP is provided to criminal investigators for unscheduled duty except for regularly scheduled overtime work as provided under 5 USC 5542, night duty, Sunday duty, or holiday duty. LEAP will be paid to criminal investigators while they attend the Criminal Investigator Training Program (CITP) at the Federal Law Enforcement Training Center (FLETC).

54.2.c. Criminal Investigator. Criminal investigator means a law enforcement officer as defined under 5 USC 5541(3) that also is required to:

54.2.c.(1). possess knowledge of investigative techniques, laws of evidence, rules of criminal procedure, and precedent court decisions concerning admissibility of evidence, constitutional rights, search and seizure, and related issues;

54.2.c.(2). recognize, develop, and present evidence that reconstructs events, sequences, and time elements for presentation in various legal hearings and court proceedings;

54.2.c.(3). demonstrate skills in applying surveillance techniques, undercover work, and advising and assisting the United States Attorney in and out of court;

54.2.c.(4). demonstrate the ability to apply the full range of knowledge, skills, and abilities necessary for cases that are complex and unfold over a long period of time (as distinguished from certain other occupations that require the use of some investigative techniques in short-term situations that may end in arrest or detention);

54.2.c.(5). possess knowledge of criminal laws and Federal rules of procedure that apply to cases involving crimes against the United States, including:

54.2.c.(5).(a). knowledge of the elements of a crime;

54.2.c.(5).(b). evidence required to prove the crime;

54.2.c.(5).(c). decisions involving arrest authority;

54.2.c.(5).(d). methods of criminal operations;

54.2.c.(5).(e). availability of detection devices; and

54.2.c.(6). possess the ability to follow leads that indicate a crime will be committed rather than initiate an investigation after a crime is committed.

54.2.d. **Unscheduled Duty.** Unscheduled duty means hours of duty a criminal investigator works, or is determined to be available for work, that are not part of the 40 hours in the basic workweek or are not scheduled overtime hours paid under 5 USC 5542.

54.2.e. **Regular Workday.** Regular workday means each day in the basic workweek during which the investigator works at least 4 hours that are not scheduled overtime hours or unscheduled duty hours.

54.2.f. **Administrative Workweek.** Administrative workweek means a period of 7 consecutive calendar days designated in advance by the head of an agency under 5 USC 6101. The DCIS administrative workweek begins on Sunday and ends on Saturday.

54.2.g. **Basic Workweek.** A basic workweek for full-time employees means the 40-hour workweek. The DCIS basic workweek is from 8:00 a.m. to 4:30 p.m., Monday through Friday. The Special Agent in Charge (SAC), Directorate head, or Resident Agent in Charge (with SAC approval) may adjust the length of the regular workday and workweek up to 10 hours per day, not to exceed 50 hours in the week. A scheduled change to the basic workweek must be

recorded in the Defense Civilian Payroll System (DCPS) BEFORE the pay period in which it goes into effect and on the DCIS Form(s) 54 affected by the change. For example, a supervisor may change the schedule of a criminal investigator from Monday through Friday, 8:00 a.m. to 4:30 p.m., to Monday and Wednesday through Saturday, 7:00 a.m. to 5:30 p.m., to ensure coverage of a Title III intercept. Since this does not exceed 10 hours per day or 50 hours per week, the employee would not be entitled to overtime. The employee would claim 10 hours of availability hours for the week.

54.2.h. Sunday Pay. Regularly scheduled work on Sundays is paid at the rate of base pay, plus 25 percent of base pay. “Regularly scheduled” means the criminal investigator’s workweek has been formally redefined to include Sunday as a regular workday. A criminal investigator that elects to work on Sunday will not be paid Sunday pay, but rather should record time on the Form 54 in the appropriate category worked and as excess LEAP hours. Overtime, not Sunday pay, is appropriate if the supervisor schedules and orders the criminal investigator to work on Sunday (for example, to ensure coverage of a Title III intercept) without submitting a formal request to change the criminal investigator’s workweek. When Sunday is not part of the regularly scheduled workday, Sunday pay is computed at 1.5 times base pay, not to exceed that of a GS-10, step 1. No employee is entitled to Sunday pay for training on Sundays.

54.2.i. Holiday Pay. An employee that is scheduled to perform work on a holiday is entitled to pay at the rate of his/her base pay, plus premium pay at a rate equal to his/her base pay, so long as the employee does not work in excess of 8 hours or the work is not scheduled overtime. A criminal investigator that ELECTS to work on a holiday will not be paid holiday pay, but rather should record time on the Form 54 in the appropriate category worked and as excess hours. Holiday pay is not payable when the employee receives training on a holiday.

54.2.j. Night Differential. Regularly scheduled work after 6:00 p.m. and before 6:00 a.m. is paid at the rate of base pay, plus 10 percent of base pay.

54.2.k. Scheduled Overtime. Criminal investigators that are on LEAP will be paid for overtime that is in excess of 10 hours on a day containing part of the basic 40-hour workweek or on a day that is not part of the basic workweek AND is SCHEDULED IN ADVANCE of the administrative workweek. Scheduled overtime is NOT counted in the computation of the 2-hour per day LEAP requirement. All other “overtime” work is considered LEAP time. Scheduled overtime is paid at the rate of 1.5 times the employee’s base pay rate if the base pay is less than or equal to GS-10, step 1. For employees whose base pay exceeds a GS-10, step 1, scheduled overtime is paid at the greater of the rate of 1.5 times a GS-10, step 1, or the hourly rate of basic pay. Criminal investigators who are on LEAP are not entitled to overtime compensation for hours worked while engaged in any type of training. Examples of overtime for criminal investigators are included in Attachment A.

54.2.l. Maximum Pay. The total of all premium pay (LEAP plus any identified in paragraphs 54.2.h. through 54.2.k.) during a pay period is limited to the amount equal to THE HIGHER OF the pay period rate payable for level V of the Executive Schedule or a GS-15, step 10, including any applicable locality-based comparability pay. The Inspector General may waive the biweekly cap for employees performing work deemed “critical to the agency’s mission” and not just in emergencies that threaten life or property. However, employees will

still be subject to a total pay cap on a calendar year basis of the higher of those two rates. Supervisors should be mindful of this limitation when scheduling overtime, holiday, Sunday, or nighttime work for their employees.

54.3. Eligibility

54.3.a. LEAP will be paid at a rate of 25 percent of basic pay to DCIS criminal investigators that certify that they expect to be “available” as defined in paragraph 54.2.b. Before being placed on LEAP, and annually thereafter, each criminal investigator must certify to his or her availability for the upcoming leave year using the format specified in Attachments B and C.

54.3.b. LEAP will commence for all GS-5 and new criminal investigators upon entry into FLETC CITP and submission of the availability statement specified in paragraph 54.3.a. LEAP will start at the beginning of the pay period in which the criminal investigator is scheduled to attend the first CITP class. Since classes always commence on a Monday, LEAP will begin either on the Sunday prior to class, or, in the case where CITP begins in the middle of a pay period, on the Sunday a week prior to class. LEAP will commence for criminal investigators transferring from another agency at GS-7 level or above upon verification that they have completed an approved basic criminal investigator training program and submission of the availability statement specified in paragraph 54.3.a. Criminal investigators, regardless of grade, that have not graduated from an approved basic training program will be required to attend the FLETC CITP. In all cases, LEAP cannot commence until personnel and payroll process the appropriate paperwork.

54.3.c. The criminal investigator will continue to receive LEAP when attending agency-sanctioned training, on agency-approved sick leave or annual leave, on agency-ordered travel status, or on excused absence with pay for relocation purposes.

54.3.c.(1). Agency-sanctioned training includes all training from outside vendors for which a DD 1556 is prepared, training provided by the OIG (such as in-services and administrative conferences), quarterly firearms re-qualifications, semiannual physical fitness testing, professional conferences, and other locally provided training when approved in advance by the criminal investigator’s supervisor.

54.3.c.(2). Agency-ordered travel status means travel to and from any event for which orders were prepared and a voucher submitted.

54.3.d. An involuntary reduction in pay resulting from a denial of certification and removal from LEAP is considered an adverse personnel action. As such, all such actions must be coordinated through the ODIG-INV Management Support Office and the Human Capital Advisory Services Directorate, Assistant Inspector General for Administration and Management.

54.3.e. All DCIS criminal investigators are eligible to receive LEAP and are exempt from the Fair Labor Standards Act (FLSA) of 1938 once LEAP begins.

54.4. General Rules

54.4.a. **Eligibility for LEAP.** A criminal investigator shall continue to be paid LEAP if the annual **daily** average of hours is equal to or greater than 2 hours for the following:

54.4.a.(1). unscheduled duty hours worked by a criminal investigator in excess of each regular workday; and

54.4.a.(2). unscheduled duty hours a criminal investigator is available to work on each regular workday upon the request of ODIG-INV management.

54.4.b. **Scheduled and Unscheduled Hours.** Unscheduled duty hours worked on days that are not regular workdays shall be considered in the calculation of the annual average of unscheduled duty hours worked or available for certification. SCHEDULED overtime and work on Sundays, holidays, and nighttime will NOT be considered in the calculation of hours for certification.

54.4.c. Credit Hours and Compensatory Time Off

54.4.c.(1). Compensation for unscheduled duty hours in excess of the annual 2-hour daily average requirement described above is NOT authorized by pay, credit hours, or compensatory time off for criminal investigators that are paid LEAP.

54.4.c.(2). For criminal investigators that are not paid LEAP, compensation for unscheduled duty hours in excess of 8 hours per day is governed by applicability of the FLSA. FLSA-covered employees are generally those paid at less than a GS-9. FLSA-exempt employees are generally those paid at GS-9 and above. Supervisors should request the employee provide a copy of his/her most recent SF-50 to determine FLSA status before scheduling work in excess of basic hours for a covered employee.

54.4.c.(2).(a). Credit hours can only be earned when an employee not on LEAP chooses to work in excess of the basic 8-hour workday. Credit hours may **NOT** be earned:

54.4.c.(2).(a).1. when the supervisor orders the employee to work in excess of the basic 8-hour workday or when the criminal investigator is required to “work” in excess of the basic 8-hour workday while attending the CITP at FLETC;

54.4.c.(2).(a).2. for work before 6:00 a.m. or after 7:00 p.m.;

54.4.c.(2).(a).3. for work on weekends or holidays; or

54.4.c.(2).(a).4. in excess of 2 hours per calendar day.

54.4.c.(2).(b). Credit hours must be earned before they can be used, even within a single pay period. Credit hours may not be used after a criminal investigator is on

LEAP, nor are credit hours counted in the calculation of the average excess hours for LEAP. Further details concerning credit hours may be found in IG Regulation 1400.610, "Alternate Work Schedules Program," January 1, 1998.

54.4.c.(2).(c). Compensatory time off applies only to criminal investigators that are covered by the FLSA.

54.4.c.(2).(c).1. If covered by the FLSA, a criminal investigator not receiving LEAP may elect to earn compensatory time off when ordered to work hours in excess of the basic 8-hour workday. A supervisor cannot order a criminal investigator not on LEAP to accept compensatory time for excess hours ordered to be worked. If the criminal investigator does not choose to accept compensatory time off, the criminal investigator must be paid overtime, plus any applicable differentials for Sunday, holiday, or night work.

54.4.c.(2).(c).2. If exempt from the FLSA, a criminal investigator not covered by LEAP may NOT earn compensatory time off when ordered to work in excess of the basic 8-hour workday. In such case, the criminal investigator must be paid overtime and any applicable differentials for Sunday, holiday, or night work.

54.4.d. Work Performed at Home

54.4.d.(1). IG Regulation 1400.620, "Office of the Inspector General, Department of Defense Telework Program," December 20, 2001, governs work performed at home during duty hours. Employees and their supervisors may make telework arrangements to promote efficiency of the Government and foster a family-friendly OIG DoD. The telework program is not an entitlement, but an individualized structured program with a formal written agreement. Telework must be voluntary, consistent with mission accomplishment, in compliance with the IG Regulation, and without diminished employee performance.

54.4.d.(1).(a). Telework does not apply to work at task force sites and day offices.

54.4.d.(1).(b). All employees scheduled to work at home or at an official telework center must complete the required telework paperwork contained in IG Regulation 1400.620 before commencing telework.

54.4.d.(2). Except for approved telework arrangements, work at home may be claimed for unscheduled duty with supervisory approval. Such situations are limited to those triggered by sources outside the OIG, such as telephone calls from Assistant U.S. Attorneys or informants. The circumstances must be noted on the Form 54 in the "Remarks" section.

54.4.d.(3). A criminal investigator that is asked by management to be available for duty during unscheduled duty hours is not required to remain in the office or at home, but must be reachable either by telephone, pager, or similar device.

54.4.e. **Overtime.** DCIS criminal investigators NORMALLY will not be assigned regularly scheduled overtime; however, they will be assigned tasks (investigations, surveys,

administrative assignments) that will likely require unscheduled duty. They will, because of their assignments, experience erratic and irregular periods of work, the nature and required duration of which cannot be determined in advance.

54.4.f. DCIS Form 54. The recording of unscheduled duty hours for annual LEAP certification purposes will be accomplished by the accurate completion of DCIS Form 54, the Biweekly Activity Report (Criminal Investigators). DCIS supervisory personnel are responsible for ensuring that criminal investigators' reports of hours of unscheduled duty hours worked or available are accurate. First line managers should CAREFULLY review the Form 54 before signing it to ensure that time charged corresponds with the work achieved during the period. Criminal investigators will report all unscheduled duty hours they were available for duty at the request of management, but did not perform duties that occur on a regular workday, as well as all unscheduled duty hours actually worked, regardless of when they occur.

54.4.g. Voluntary Opt-Out

54.4.g.(1). It is recognized that a criminal investigator may not be able to perform official duties during unscheduled duty hours or generally be available to the extent required by this chapter for a designated period of time. This time period generally will be more than 1 month. The criminal investigator, with supervisory approval, may opt out at any time by signing a memorandum documenting the request and his/her understanding that LEAP will not be paid during the designated period. A sample opt-out certification is shown at Attachment C. Upon expiration of the designated period, the criminal investigator will be placed on LEAP effective at the beginning of the pay period following the period designated.

54.4.g.(2). Criminal investigators that opt out will establish a gliding schedule for their work hours and will be compensated by credit hours for any unscheduled hours that may be worked. However, credit hours cannot be worked outside the credit hour time bands within the OIG DoD, which are 6:00 a.m. to 9:00 a.m. and 3:00 p.m. to 7:00 p.m., Monday through Friday, excluding holidays. Regulations on the accumulation and use of credit hours are defined in IG Regulation 1400.610. Credit hours worked and taken must be reported on DCIS Form 54 and through the biweekly submission of payroll to the DCPS.

54.4.g.(3). A criminal investigator that opts out will normally not work unscheduled hours outside his/her gliding schedule. In those instances when it is required, advance written supervisory approval must be obtained. The criminal investigator may request compensatory time off for hours worked during hours outside his/her gliding schedule. Otherwise, overtime must be approved in advance for such work. Compensatory time worked and taken must be reported on DCIS Form 54 and through the biweekly submission of payroll to DCPS.

54.4.h. Revoking Certification. A SAC/Headquarters (HQ) Director may propose revoking a criminal investigator's certification at any time based on a finding that, due to changed circumstances (e.g., the avoidance of work or nonavailability by the criminal investigator), the criminal investigator is expected to no longer meet the average 2 hours per day

requirement. Any revocation of an originally valid certification will be made on a prospective basis and will result in removal from LEAP. Such actions will be handled under adverse action procedures.

54.4.i. Outside Employment. Requests for approval of outside employment or other activities for which the criminal investigator receives compensation or benefits will be considered only where the criminal investigator can show that such employment or activity will not interfere with his/her ability to be available, and after having been reviewed per IG Policy Memorandum 2006-6, "Policy on outside employment and business activities," March 6, 2006. The Guidelines for the Exercise of Law Enforcement Authorities by Special Agents of the Defense Criminal Investigative Service prescribed by the Inspector General of the Department of Defense and approved by the Attorney General pursuant to 10 USC 1585a prohibit special agents from being cross-designated or deputized as state or local officers unless the Director, DCIS, determines that such cross-designation or deputation is essential to the performance of agency responsibilities. Therefore, special agents may not seek outside employment in a law enforcement capacity.

54.5. Reporting Requirements

54.5.a. Biweekly Activity Report, DCIS Form 54. Completion of the Biweekly Activity Report, DCIS Form 54, will be the only reporting requirement for criminal investigator personnel to track hours worked for LEAP. Use and preparation of the DCIS Form 54 is explained in paragraph 54.6.

54.5.b. Initial Certification. The SAC or HQ Director will certify to the Director, DCIS, that a newly hired criminal investigator is a graduate of an approved criminal investigator basic training program or is anticipated to begin the CITP class, and therefore expected to meet the LEAP requirements of this chapter. A sample certification is shown as Attachment B. This certification will authorize the payment of LEAP to the criminal investigator. The criminal investigator must also complete the individual certification specified in paragraph 54.3.a. These documents must be received and processed through personnel and payroll before LEAP can be paid.

54.5.c. Annual Certification of Availability Hours

54.5.c.(1). Each criminal investigator must complete a Special Agent Annual/Opt-Out Certification memorandum (Attachment C) each year and provide it to his/her SAC. Each SAC/HQ Director will conduct an annual review of qualification for LEAP using one of the LEAP Hour reports in the IDS - Workhour Tracking System (WTS) module, and provide a certification memorandum (Attachment D) to the Director, DCIS, through the Information Analysis Branch, Internal Operations Directorate. The certification must specify that the criminal investigators have met and are expected to continue to meet the requirements of this chapter. The annual certifications will be prepared on a leave year basis. Annual individual criminal investigator certifications are due to the SAC by January 20, and the SAC certifications are due to the Internal Operations Directorate by January 25.

54.5.c.(2). Criminal investigators that do not meet the annual requirement for LEAP will be proposed for removal from LEAP. Such proposal will be handled as an adverse action.

54.5.d. Quarterly Availability Hours Audit

54.5.d.(1). Because of varying situations, confirmation of an employee's eligibility for LEAP over short periods, such as a pay period or any given month, could be difficult. To ensure that the employee maintains qualification for LEAP, immediate supervisors will conduct an audit at least quarterly for all their employees on LEAP. The audit may be conducted by running the LEAP Report by Agent or the LEAP Report by Office through the reports module of the Investigative Data System (IDS). See Attachment E or SAM Chapter 50 for instructions on how to run these reports.

54.5.d.(2). Since the quarterly audit of an individual's qualification for LEAP is "after the fact," it may show that the employee did not meet the required daily 2-hour average minimum of unscheduled duty per week for that quarter. The manager should advise the criminal investigator that he/she is in danger of not meeting the annual qualification for LEAP. The manager and the employee are responsible for establishing a course of action to ensure that the individual will meet the annual qualification. The SAC or appropriate HQ Director should review the circumstances and reasons for not meeting this requirement.

54.6. Biweekly Activity Report, DCIS Form 54

54.6.a. **DCIS Form 54.** The Biweekly Activity Report, DCIS Form 54, is designed to document work time and attendance hours for all criminal investigator personnel, except Senior Executive Service, regardless of assignment or organizational level. It provides a system for collecting and reporting criminal investigator hours and is used by management to compute costs of investigative efforts (for recovery of investigative costs), measure organizational productivity, determine eligibility for LEAP, and other management information requirements. (See S:\DCIS\ Form 54 Master.xls, for an electronic copy of the DCIS Form 54) Use of the DCIS Form 54 is optional for other ODIG-INV employees, as determined by the employee's manager. For example, the Form 54 could be used to track administratively uncontrollable overtime by nonagent personnel.

54.6.b. **Criminal Investigators' Responsibilities.** Criminal investigators and other employees designated by their manager shall complete individual Biweekly Activity Reports for each reporting period, as defined in paragraph 54.6.e.(1). The Common Access Card may be used to digitally sign an e-mail transmitting an attached electronically generated Form 54 without printing or signing a paper copy of the form. In lieu of using the Common Access Card, criminal investigators may submit electronically created Forms 54 to the supervisor as an attachment to a regular e-mail, as long as the body of the e-mail has a statement similar to the following: "I certify that the attached Form 54 is a true and correct reflection of the original." Criminal investigators that use paper Forms 54 must sign the form before submitting to the supervisor.

54.6.c. **Supervisors' Responsibilities.** Besides completing and signing their own individual reports, as required in paragraph 54.6.b, supervisors will review reports submitted by

subordinate criminal investigators, approving those criminal investigators' unscheduled duty hours. Supervisors may approve digitally signed and submitted Forms 54 by responding to the criminal investigator with a digitally signed e-mail and forwarding the attachment to the administrative person responsible for making DCPS and WTS entries. Supervisors are not required to print or sign a paper copy of the form that has been transmitted via digitally signed e-mail. Manually created (paper) Forms 54 must be signed by the supervisor. Supervisors will ensure that all appropriate information has been entered into the automated WTS module of the IDS.

54.6.d. Administrative Personnel Responsibilities. Support personnel will enter information from the Forms 54 into the WTS module of IDS, print, and retain electronic Forms 54 with all transmittal and approving e-mails, DCPS Master Time History, leave forms, and any other pertinent documentation.

54.6.e. Preparation of Individual Reports

54.6.e.(1). Entries on the Biweekly Activity Report, DCIS Form 54, will be computer-generated (the preferred method), typed, or handwritten in ink. The reporting period will correspond to official pay periods. Pay periods end on alternate Saturday nights at midnight. All signed DCIS Forms 54 must be provided to the supervisor no later than 2 business days following the pay period ending date. When a criminal investigator transfers from one DCIS office to another, coordination must take place between the losing office and the gaining office to ensure continuous coverage in the WTS module. Criminal investigators who begin working for DCIS or who depart DCIS during a pay period will complete a Form 54 for the entire pay period, regardless of date reported or departed. For example, a new criminal investigator reporting on the second Tuesday of the pay period, whose basic workweek is Monday through Friday, will charge 8 hours Leave-Other (Excludable Days) for the entire first week of the pay period, plus the second Monday of the pay period. A criminal investigator who departs DCIS on the same date will charge 8 hours Leave-Other (Excludable Days) for the last 4 days of the pay period.

54.6.e.(2). Time reported under the various categories will be rounded to the nearest quarter hour. Enter the appropriate dates directly under the preprinted days of the week in the heading of the form.

54.6.e.(3). After making the final entry for the pay period, total each horizontal line and enter the sum in the total column. (The electronic version of the Form 54 performs all calculations automatically.)

54.6.e.(4). Any credit hours claimed or taken, scheduled overtime, or scheduled night, holiday, or Sunday hours must be reported by actual clock hours on the back of the form.

54.6.e.(5). Time actually spent traveling outside the regular workday or basic workweek may be claimed as unscheduled duty hours. The time actually spent in agency-ordered travel status should be charged to the activity to which the travel is associated. For example, a criminal investigator spends 4 hours traveling to FLETC to attend CITP. Four hours travel time should be shown on Sunday under category "G" Training (see paragraph 54.6.g.(7)). When agency-ordered travel of 4 hours or more occurs on a regular business day, the day is

“excludable,” as discussed in paragraph 54.6.g.(17).[Q.]. When this occurs, the criminal investigator should provide an explanation in the “Remarks” portion of the Form 54. Where a criminal investigator, for reasons of personal convenience, is authorized to travel under the “constructive cost method,” the amount of travel time that may be claimed is limited to the amount he/she would be allowed if he/she had used the carrier (airplane, train, etc.) upon which constructive transportation costs are determined. Additional examples of handling travel time are given in Attachment F.

54.6.f. **DCIS Form 54 Headings.** The heading items on the electronic Form 54 can be completed once and then saved to avoid repetitive input for successive pay periods. Heading items will be completed as follows.

54.6.f.(1). **Name.** Enter last name, first name, and middle initial.

54.6.f.(2). **Grade.** Enter the GS grade level. Do not include any corresponding step level.

54.6.f.(3). **ID #.** Enter criminal investigator’s identification number. This is the criminal investigator’s IDS Userid, consisting of the last name initial plus the last four digits of the Social Security Number. NOTE: IDS Userid’s are not changed when an employee’s name changes due to marriage, divorce, etc.

54.6.f.(4). **Reporting Period From/To.** Enter the pay period beginning and ending dates.

54.6.f.(5). **Office.** Enter the four-character DCIS alphanumeric code for the office to which the criminal investigator is assigned.

54.6.f.(6). **Availability Pay.** Place an “X” in the appropriate box to reflect whether the criminal investigator is receiving LEAP.

54.6.f.(7). **Position.** Place an “X” in the appropriate block to show nature of duties:

54.6.f.(7).(a). HQ - Headquarters staff (including criminal investigators on special assignment to Headquarters);

54.6.f.(7).(b). Field Mgr - Special Agents in Charge, Assistant Special Agents in Charge, Resident Agents in Charge, and Group Managers; or

54.6.f.(7).(c). Agent - Includes all other criminal investigators.

54.6.f.(8). **Basic Work Week Days.** Enter the three-character day of the week on which the criminal investigator’s basic workweek begins (FROM) and ends (TO) using the abbreviations SUN, MON, TUE, WED, THU, FRI, or SAT.

54.6.f.(9). **Hours.** Enter the four-digit hours of the day to indicate the criminal investigator’s basic work hours (FROM) and (TO) using 0001 for 12:01 a.m. through 2400 for

midnight in a 24-hour period. Include in the basic workweek hours the criminal investigator's lunch period. For those criminal investigators who work a gliding schedule, enter the word "Gliding."

54.6.g. **Activities.** Enter the four-digit hours of the time the workday begins and ends in the Time In/Time Out Fields. Use colons and the 24-hour clock, e.g., 06:45 or 16:30. The body of the Form 54 identifies the various activities that normally are performed by DCIS criminal investigators. All time will be reported to the nearest quarter hour. Enter the number of hours on the appropriate line under the day on which the activity is performed. NOTE: The lettered paragraphs below correspond to the lettered lines on the Form 54.

54.6.g.(1). **[A.] Investigations UID.** In this column list the Unique Identifier (UID), e.g., 9410001Y or 200000026Z. Under each date, report any investigative effort, including travel, report writing, file review, time spent in court, etc., that is directly related to that case. Time expended on fraud awareness briefings and information reports should also be reported in this section. Show the number of hours expended in each 24-hour period for each UID.

54.6.g.(2). **[B.] Case Development.** Until such time as the WTS module accepts individual Case Development Package (CDP) numbers, use this line to report the aggregate number of hours expended on case development activity. Once a UID has been assigned to the activity, charge time to the UID according to the preceding paragraph.

54.6.g.(3). **[C.] Availability Hours.** Use this line to report unscheduled hours during the regular workweek for which an employee was requested by management to be available (e.g., in a "standby" mode or when assigned as the duty agent) BUT DID NOT ACTUALLY PERFORM DUTIES. Do not use this line for unscheduled hours not actually worked that occur outside of the regular workweek (e.g., weekends and holidays). An explanation of the activity requested by management must be recorded in the "Remarks" section of the form.

54.6.g.(4). **[D.]** Not currently used.

54.6.g.(5). **[E.] Liaison.** Use this line to report time spent meeting with Federal, state, and local agencies to encourage cooperation, enforcement of state laws, or the exchange of resources. Also use this line to report activities such as time spent in law enforcement "torch runs" in support of the Special Olympics. Liaison time is different than case development time in that it is a "meet and greet" general discussion category. If specifically identifiable investigative actions arise as a result of the liaison, report the specific actions under "Case Development." Include in "Liaison" any travel time related to the activity. Unscheduled duty hour time may be charged to this category only with prior supervisory approval, and an explanation of the liaison activity performed must be reflected in the "Remarks" section of the form.

54.6.g.(6). **[F.]** Not currently used.

54.6.g.(7). **[G.] Training (received or provided).** Enter the time expended while in training or in developing job-related skills; participating in firearms familiarization or

qualification; courses taken on official time at non-Government institutions; time expended in the preparation, presentation, and evaluation of training programs administered to DCIS criminal investigators or other personnel; and all time associated with the semiannual physical fitness test (this time is not counted against the 4 hours a week maximum associated with regular physical fitness activities (see paragraph 54.6.g.(9).[I.]). Include related travel time. Training of 4 or more hours that occurs on a basic workweek day is an excludable day (see paragraph 54.6.g.(17).[Q.]). Criminal investigators attending the FLETC CIP should record all actual training hours in this category. (NOTE: Record time expended in on-the-job training under the actual activity being performed. Time spent on fraud briefings should be charged as direct effort to a briefing UID under paragraph 54.6.g.(1).[A.] This section does NOT apply to DCIS employees that are permanently assigned or on detail to FLETC or the IG Academy with teaching or training as their primary responsibility.)

54.6.g.(8). [H.] Not used.

54.6.g.(9). **[I.] Physical Fitness Training.** Report duty hours spent performing agency-permissible physical fitness maintenance or improvement activities (PT), up to the maximum permissible 4 hours per week in this category (see Special Agents Manual (SAM) Chapter 58). On holidays or when a criminal investigator takes a day of leave, physical fitness exercise may NOT be counted on the Form 54 as excess hours for that day, as performing PT on a holiday or an approved day of leave does not meet the substantial hours requirement of 5 CFR 550.183. Likewise, criminal investigators may not claim 1 hour of PT in combination with 7 hours leave; instead, they must take 8 hours leave.

54.6.g.(10). **[J.] Administration**

54.6.g.(10).(a). Headquarters staff and field supervisory personnel will report the hours expended on supervisory, management, support, and staff activities in this category. DCIS employees that are assigned (on detail or permanently) at FLETC or the IG Academy with teaching or training as their primary responsibility should charge their hours for preparation, teaching, or training to this category.

54.6.g.(10).(b). Nonsupervisory personnel will use this category to report time expended on administrative and logistical activities such as preparing non-investigative reports and studies, maintaining official automobiles and equipment, attending staff meetings, etc. Time expended writing reports for CDPs or UIDs should be charged in A, "Investigations UID" or B, "Case Development."

54.6.g.(11). **[K.] Leave.** Enter the total daily number of hours of leave taken. Attach Form OPM-71 to the Form 54 for all leave taken. Explain entries for other leave in the "Remarks" section of the form. When a criminal investigator takes military leave, the weekend days of military leave should NOT be counted as leave time on the Form 54, in WTS, or in DCPS. Additional guidance can be found at <http://www.opm.gov/oca/leave/HTML/military.htm>. Leave of 4 or more hours on a basic workday makes the day excludable.

54.6.g.(12). **[L.] All Other (holidays, comp/credit hrs taken).** All time reported in this category, other than holidays, should be explained in the “Remarks” section of the form. Examples include jury duty and Government-ordered office closure due to inclement weather.

54.6.g.(12).(a). Report time unaccounted for in activities A through K in this category. Enter 8 for holidays falling on a workday (Monday-Friday). For criminal investigators that take time off for relocation purposes (house hunting, relocation travel) enter each day taken as 8. For criminal investigators that opt out of LEAP, enter 8 credit hours taken as 8. Holidays and relocation travel are excludable days.

54.6.g.(12).(b). Time off awards should be entered on this line. If the time off award is 4 hours or more, the day is excludable.

54.6.g.(12).(c). Leave without pay (LWOP) and unpaid time for employees because of disciplinary action should be charged against category “L”—All Other Activities—on the Form 54. Unpaid time off is excludable.

54.6.g.(12).(d). As noted in paragraph 54.6.e.(1)., use this category to reflect days before an initial DCIS reporting date for new hires or after the last reporting date for retirements and departures from DCIS when the beginning or ending date of DCIS employment does not coincide with the beginning or end of a pay period. These should be shown as excludable days.

54.6.g.(13). **[M.] Total Hours.** Enter total hours for activities A through L for each day. (The electronic version of Form 54 automatically computes total hours.)

Example: On Thursday of the second week, 4.0 hours were spent receiving training and entered in line H, 1 hour of PT entered in line I, and 5.25 hours were spent reviewing records connected with a particular case and entered along with the UID in Section A. The daily total (line M) would be entered as 10.25 hours. Since 2.25 hours of this total are excess over basic work hours, the number 2.25 is entered in line N, Excess Over Basic Work Hours. The day is also excludable because 4 hours were spent receiving training.

54.6.g.(14). **[N.] Excess Over Basic Work Hours (LEAP agents only).** Compute the daily total of excess hours and enter this figure under the appropriate day on line N. (The electronic version of Form 54 automatically computes excess hours.) Normally, criminal investigators will not work excess hours on an excludable day. However, supervisors may review and approve such claims in exceptional cases.

Example 1: A criminal investigator works 4 hours on a holiday in preparation for a trial. The criminal investigator will show 4 hours associated with the case UID in line A, 8 hours associated with the holiday in line L, 12 total hours in line M, 4 excess hours in line N, and 1 excludable day in line Q.

Example 2: Excess work performed in the evening after a full day of training would be counted as excess hours and the day would be excludable.

54.6.g.(15). **[O.] Scheduled Overtime.** Enter the clock hours on the reverse side of the form of any officially ordered and approved overtime worked. Compute the daily number of hours and enter the total for the appropriate day in this activity. The Director, DCIS, must approve all scheduled overtime in advance. If approved, include night, holiday, and Sunday hours. **DO NOT REPORT SCHEDULED PAID OVERTIME AS EXCESS OVER BASIC HOURS IN PARAGRAPH 54.6.g.(14).[N.].** The WTS makes this adjustment automatically.

54.6.g.(16). **[P.] Credit Hours Worked (no LEAP agents).** For criminal investigators that do not receive LEAP, enter the total credit hours worked on this line and on the reverse of the form. No more than 2 credit hours may be earned per calendar day, and no more than 24 credit hours earned may be carried from one pay period to the next. Do not report credit hours worked as Excess Over Basic Hours in line N, above. Credit hours cannot be earned before 6:00 a.m., or after 7:00 p.m., or on weekends, and they cannot be used before being earned, even within a pay period.

54.6.g.(17). **[Q.] Excludable Days (LEAP agents only).** Place a “1” on this line under each excludable day. (The electronic Form 54 automatically computes excludable days.) Do not place a “1” on this line for Saturday or Sunday unless the supervisor has changed the basic workweek to include Saturday or Sunday, as specified in paragraph 54.2.g., and the aforementioned excludable day conditions apply. The total number of excludable days shall be entered in the “TOTALS” column on line Q. An “excludable day” is any day in which the combination of the following equals 4 or more hours:

54.6.g.(17).(a). all leave, including LWOP;

54.6.g.(17).(b). training (received or provided);

54.6.g.(17).(c). any holiday;

54.6.g.(17).(d). time off award taken;

54.6.g.(17).(e). was in transit on agency-ordered travel (see Attachment F for examples of handling travel time as excludable days); or

54.6.g.(17).(f). was excused from work for relocation purposes (house hunting, travel to new duty station, etc.).

54.6.g.(18). **[R.] Telecommute Days (Mark with “TW”).** Place “TW” on this line under each day on which work was performed at an approved telecommute or telework site.

54.6.g.(19). **[Remarks.]** Enter any comments that would explain unusually high totals in any given category (FLETC, Office of Personnel Management training, HQ details, etc.) or as specified in the above paragraphs.

54.6.h. Signature and Approvals. Criminal investigators that create paper Forms 54 will sign the Form 54 and submit it to their supervisor within 2 workdays following the close of each reporting period. When submitted with a digital signature using the Common Access Card, criminal investigators may submit electronically created Forms 54 to the supervisor as an attachment to an e-mail without printing and signing them by hand. In lieu of using the Common Access Card, criminal investigators may submit electronically created Forms 54 to the supervisor as an attachment to a regular e-mail, as long as the body of the e-mail has a statement similar to the following: "I certify that the attached Form 54 is a true and correct reflection of the original." Supervisors will review forms within 4 workdays following the close of each reporting period. If approved, supervisors will sign paper forms in ink and sign electronic forms by attaching them to a digitally signed e-mail or printing the e-mail and Form 54 attachment, signing the paper Form 54, and submitting the form with the e-mail. Inaccurate or incomplete forms will be returned to the criminal investigator for correction and resubmission within 5 workdays following the close of each reporting period.

54.6.i. Form Distribution. The original paper form or final printed version of an electronic form will be used to enter information into the automated WTS and DCPS. It will be retained in the field office with the DCPS Master Time History report, leave request forms, and any other pertinent documentation. Forms 54 for all SACs and HQ Directors will be submitted to and approved by the Deputy Director, DCIS. The SACs' Forms 54 will be returned and stored at the field office. Records will be destroyed 6 years after the end of the fiscal year for the time documented.

54.7. Workhour Tracking System (WTS)

54.7.a. The automated WTS will be used to capture work hours of all criminal investigator personnel assigned to DCIS. Entry of information into the system is done at the local office level, using information contained on the Form 54. Details on how to make specific entries in the WTS are contained in Attachment E and in SAM Chapter 50.

54.7.b. Entry of information from the manager-approved Form 54 into the WTS will be done at the local office level not later than 5 workdays following the close of each reporting period.

54.7.c. The WTS also includes a variety of standard reports for use by DCIS managers. It is important to note that all LEAP Hour reports are calculated on the leave year, not the calendar or fiscal year. When running these reports, the "BEGIN DATE" field must be the pay period beginning date, and the "END DATE" field must be the pay period ending date in order for the information in the reports to be accurate. WTS reports include the following:

54.7.c.(1). Individual Agent Activity Report. Provides summary information, by type of activity and case number, on hours charged by an individual criminal investigator during any specified report period.

54.7.c.(2). Individual Office Activity Report. Provides summary information, by type of activity and case number, on hours charged by an office during any specified report period.

54.7.c.(3). **Combined Office Activity Report.** Contains listings of all activity totals, during any specified reporting period, for each criminal investigator within a group of offices (usually a field office). This report also contains an office summary by activity; however, it does not break down investigative hours by case number.

54.7.c.(4). **LEAP Hour Report by Office.** Reports all unscheduled duty hours worked or available and excludable days by criminal investigator during any specified reporting period. NOTE: SACs and DCIS HQ supervisory personnel may use this report to satisfy the annual certification of eligibility for LEAP. However, SACs and DCIS HQ supervisory personnel must submit a separate certification of eligibility for availability hours.

54.7.c.(5). **LEAP Hour Report by Agent.** Reports all unscheduled duty hours worked or available and excludable days for a specified criminal investigator during any specified reporting period. This report is useful for criminal investigators and supervisors to verify that the criminal investigator is on track to meet the annual LEAP requirement, and is particularly helpful when a criminal investigator has transferred between two offices during the reporting period.

54.7.c.(6). **LEAP Hour Summary Report for All Agents.** Reports a summary for all criminal investigators of the number of work hours, excludable days, adjusted work days, excess hours worked, and the average number of excess hours worked for the time period requested. If the average number of excess hours worked is less than 2.0, the number will be highlighted in red.

ATTACHMENTS

- A Examples Involving Scheduled Overtime
- B Initial Certification Memorandum
- C Special Agent Annual/Opt-Out Certification Memorandum
- D Annual Certification Memorandum
- E Instructions for Use of WTS and WTS Reports
- F Examples of Excludable Days – Travel Time

ATTACHMENT A

EXAMPLES INVOLVING SCHEDULED OVERTIME

1. A criminal investigator is scheduled to work from 1600 hours to 0400 hours Monday through Friday. The criminal investigator then works 8 hours unscheduled time on Saturday. Since “scheduled” means the basic workweek was established **prior** to the beginning of the administrative workweek (i.e., not later than the Saturday before the Sunday beginning the administrative workweek in question), the criminal investigator would be paid his/her regular pay from 4:00 p.m. to 6:00 p.m., then night differential from 6:00 p.m. to 4:00 a.m. In addition, the criminal investigator would receive overtime from 2:30 a.m. to 4:00 a.m. Computation of the overtime rate does not include the night pay differential. The criminal investigator must work 10 hours on a regular workday before he/she is eligible to be paid overtime pay. This requirement is automatically incorporated into the WTS data entry screen. Since the 8 hours worked on Saturday are unscheduled, the criminal investigator will use those excess hours in the calculation of annual average LEAP certification.
2. A criminal investigator is scheduled to work from 1600 hours to 0400 hours, Saturday through Wednesday. If we are to assume that the first Saturday of this schedule was not scheduled prior to the beginning of the normal administrative workweek (Sunday through Saturday), the criminal investigator’s time for this first Saturday would not count as overtime or night pay differential, but would count toward excess LEAP hours. Assuming the Sunday through Wednesday workdays are scheduled prior to the beginning of the administrative workweek, the criminal investigator is entitled to night differential between the hours of 6:00 p.m. and 4:00 a.m. Overtime would be applied to work performed in excess of 10 hours on a day that is part of the basic 40-hour workweek (i.e., Sunday – Wednesday in this example) or on a day that does not contain hours that are part of the basic 40-hour workweek. Since the basic workweek began on Sunday, the criminal investigator must work on Thursday to complete his or her basic workweek requirement and then could have the ensuing Friday and Saturday as his/her days off.
3. A criminal investigator can be directed to work 6 or 7 consecutive days per week, although this is not the norm. Overtime would be authorized **IF** the work was scheduled in advance of the administrative workweek (i.e., not later than the Saturday before the Sunday beginning the administrative workweek in question) and the actual work is either in excess of 10 hours on a day containing hours that are part of the criminal investigator’s basic 40-hour workweek or on a day that does not contain hours that are part of his/her basic 40-hour workweek.



ATTACHMENT B
INITIAL CERTIFICATION

Investigations

MEMORANDUM FOR DIRECTOR, DEFENSE CRIMINAL INVESTIGATIVE SERVICE
THROUGH INFORMATION ANALYSIS BRANCH, INTERNAL OPERATIONS
DIRECTORATE

SUBJECT: Initial Certification of Availability Hours

I certify that Special Agent Jane Smith is expected to perform official duties during unscheduled duty hours or will be available to perform those duties during unscheduled duty hours for the remainder of the fiscal year. Special Agent Jane Smith should be placed on availability pay.

John B. Doe
Special Agent in Charge
Anywhere Field Office



Investigations

ATTACHMENT C

SPECIAL AGENT ANNUAL / OPT-OUT CERTIFICATION

MEMORANDUM FOR SPECIAL AGENT IN CHARGE, XX FIELD OFFICE

SUBJECT: Availability Pay

[☐] I, Special Agent Jane Smith, certify that I expect to be able to perform official duties during unscheduled duty hours and agree to be available for unscheduled duty based on the needs of the Inspector General, Office of the Deputy Inspector General for Investigations, as outlined in Chapter 54 of the Special Agents Manual.

[☐] I, Special Agent Jane Smith, advise you that for the period _____ through _____, I do not expect to be able to perform official duties during unscheduled duty hours or to be available for unscheduled duty based on the needs of the Inspector General, Office of the Deputy Inspector General for Investigations, as outlined in Chapter 54 of the Special Agents Manual. I understand that I will not be paid "availability pay" and that the nonpayment of availability pay is not an adverse action taken by management.

Jane Smith
Special Agent



ATTACHMENT D
ANNUAL CERTIFICATION

Investigations

MEMORANDUM FOR DIRECTOR, DEFENSE CRIMINAL INVESTIGATIVE SERVICE
THROUGH INFORMATION ANALYSIS BRANCH, INTERNAL OPERATIONS
DIRECTORATE

SUBJECT: Annual Certification of Unscheduled Duty (LEAP) Hours – Leave Year 20XX

The personnel listed in the attached report performed official duties during this past leave year (January XX, 20XX, through January XX, 20XX) during unscheduled hours of duty and were qualified for availability pay in accordance with the Availability Pay Act of 1994 and Chapter 54 of the DCIS Special Agents Manual.

By this report, I certify the criminal investigators listed in the attached report were under my supervision during this reporting period and in accordance with requirements of their official duties, performed work during unscheduled hours of duty or were available to work during unscheduled hours of duty and qualify for availability pay. I also certify that the criminal investigators listed in the attached report are expected to continue to meet these requirements.

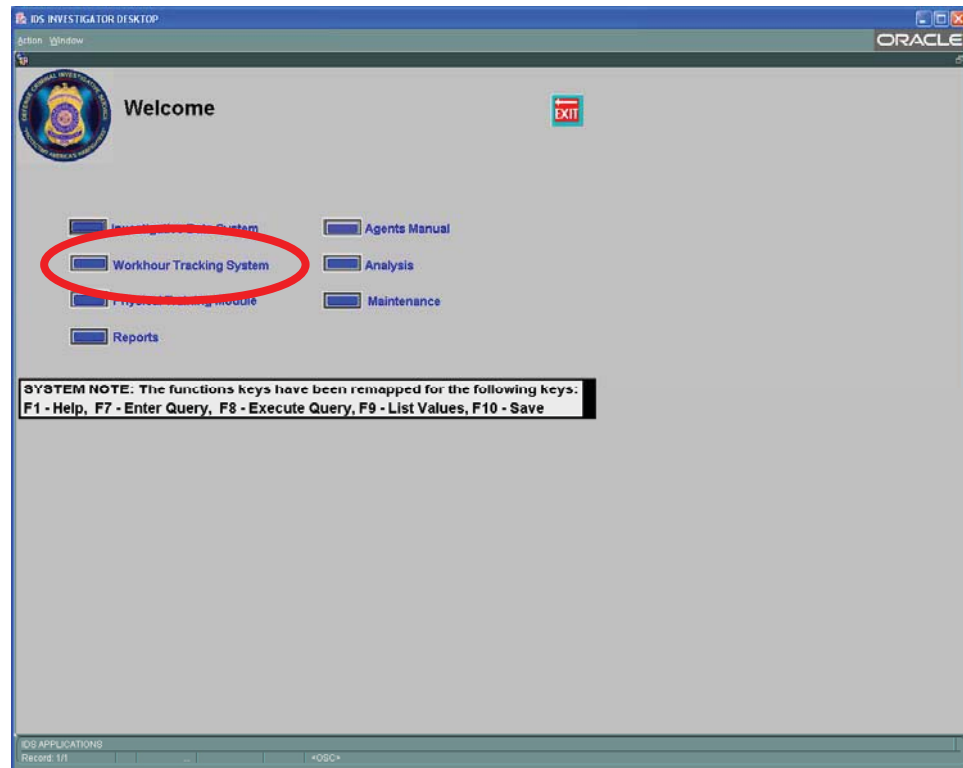
John Doe
Special Agent in Charge
Nowhere Field Office

Attachment
Unscheduled Duty Hours (LEAP) Report

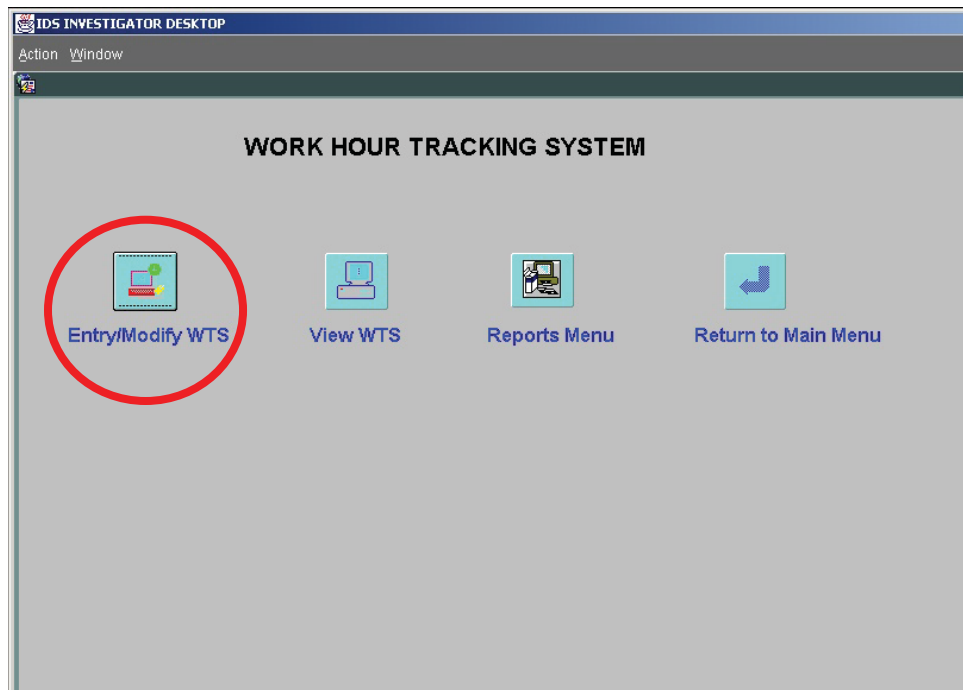
ATTACHMENT E

INSTRUCTIONS FOR USE OF WTS AND WTS REPORTS

Open IDS. Select the Workhour Tracking System icon from the Welcome screen.



Select the Entry/Modify WTS icon.



From the blank form that appears, select the icon with the clock and calculator.

[illegible]

Use the page down key on the keyboard or the scrollbar on the screen to find the desired criminal investigator name. Click the yellow button next to the name to select it.

IDS INVESTIGATOR DESKTOP - [WTS_WINDOW]

ACTION QUERY RECORD HELP EXIT Window

Agent IDNO Agent Office Agent Series Agent Grade PPE Date BASIC HOURS:

Agent Last Name:

Work Start Day:

Work Start Time:

AGENT V

Investigation Totals:

Case Development:

Available Hours:

Liasion:

Training Provided:

Training Received:

PT Training:

Administrative:

Leave:

Others:

Total Hours:

ADD AGENT TO PAY PERIOD

Agent IDNO	Agent First Name	Agent Last Name	Agent Office
			30DA
			03AA
			40MN
			04HL
			60DC
			00CF
			00CF
			60RM
			40SL
			04HL

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

Click button next to Agent IDNO to insert WTS data sheet.

CLOSE

UPDATE

Record: 1/2

Basic criminal investigator information will be added to the top of the form.

[illegible]

Click the yellow PPE button to get a list of pay period end dates. Use the scroll bar or down arrow to select the desired date and click OK.

[illegible]

UIDs of open cases assigned to the selected criminal investigator will be automatically added. Use the mouse or down arrow to add other UIDs, if applicable.

The screenshot shows the 'IDS INVESTIGATOR DESKTOP - [WTS_WINDOW]' interface. At the top, there's a menu bar with 'ACTION', 'QUERY', 'RECORD', 'HELP', 'EXIT', and 'Window'. Below the menu is a toolbar with icons for 'ACTION', 'QUERY', 'RECORD', 'HELP', 'EXIT', and 'Window'. The main area is divided into two sections: 'AGENT WORK HOUR DETAILS' on the left and 'INVESTIGATIONS' on the right. The 'AGENT WORK HOUR DETAILS' section contains various input fields for hours, including 'Investigation Totals', 'Excess Hours', 'Case Development', 'Scheduled Overtime', 'Available Hours', 'Credit Hours', 'Liasion', 'Excludable Days', 'Training Provided', 'Training Received', 'PT Training', 'Administrative', 'Leave', 'Others', and 'Total Hours'. The 'INVESTIGATIONS' section contains a table with 'UID Number' and 'Total Hours' columns. The first row shows '(b)(7)(E)' in the 'UID Number' column and '1' in the 'Total Hours' column. A red circle highlights the '(b)(7)(E)' entry. At the bottom right of the 'INVESTIGATIONS' section is an 'UPDATE' button. The status bar at the bottom shows 'Record: 2/2' and 'List of Values'.

If you add an incorrect UID, a lookup table will appear from which to select a valid UID. You cannot enter a UID that does not exist in IDS. If you omit the letter suffix, WTS will add the correct one for you. When all UID hours are input, click the Update button in the lower right corner of the screen.

This screenshot shows the same 'IDS INVESTIGATOR DESKTOP - [WTS_WINDOW]' interface as the previous one, but with a 'UID NUMBER' dialog box open. The dialog box has a 'Find' field with a '%' symbol, a list box containing '(b)(7)(E)', and 'Find', 'OK', and 'Cancel' buttons. The 'INVESTIGATIONS' table in the background now shows two rows, both with '(b)(7)(E)' in the 'UID Number' column and '1' in the 'Total Hours' column. The status bar at the bottom shows 'Choices in list: 21690', 'Record: 2/2', and 'List of Values'.

If you accidentally move your cursor to the next blank row and don't need to add another UID, or if you want to "erase" a bad record, highlight it. Then, from the menu bar, select Record|Remove Record.

The screenshot shows the 'IDS INVESTIGATOR DESKTOP - [WTS_WINDOW]' application. The menu bar includes 'ACTION', 'QUERY', 'RECORD', 'HELP', 'EXIT', and 'Window'. The 'RECORD' menu is open, and the 'REMOVE RECORD' option is highlighted with a red circle. Below the menu bar, the 'Agent Information' section displays fields for Agent ID, Office, Series, Grade, PPE Date, and Basic Hours. The 'AGENT WORK HOUR DETAILS' section includes fields for Investigation Totals, Excess Hours, Case Development, Scheduled Overtime, Available Hours, Credit Hours, Liasion, Excludable Days, Training Provided, Training Received, PT Training, Administrative, Leave, Others, and Total Hours. The 'INVESTIGATIONS' section features a table with columns for UID Number and Total Hours, and an 'UPDATE' button.

Move the cursor to the Agent Workhour Details Section and add hours as shown on the Form 54. You must add excludable days, if any.

The screenshot shows the 'IDS INVESTIGATOR DESKTOP - [WTS_WINDOW]' application. The 'AGENT WORK HOUR DETAILS' section is highlighted with a red circle. The 'INVESTIGATIONS' section is also visible. The 'AGENT WORK HOUR DETAILS' section includes fields for Investigation Totals, Excess Hours, Case Development, Scheduled Overtime, Available Hours, Credit Hours, Liasion, Excludable Days, Training Provided, Training Received, PT Training, Administrative, Leave, Others, and Total Hours. The 'INVESTIGATIONS' section features a table with columns for UID Number and Total Hours, and an 'UPDATE' button.

Save the record. Use the icon or the menu bar.

The screenshot shows the 'IDS INVESTIGATOR DESKTOP - [WTS_WINDOW]' application. The menu bar includes ACTION, QUERY, RECORD, HELP, EXIT, and Window. The toolbar contains icons for ESCAPE, SAVE, PRINT, and EXIT. The 'SAVE' icon is circled in red. Below the menu bar, there are fields for Agent Office (04PR), Agent Series (1811), Agent Grade (14), PPE Date (20-NOV-1999), and BASIC HOURS (80). The Agent Last Name and Agent First Name fields are both redacted with (b)(6), (b)(7)(C). The Work Start Day is MON, Work End Day is FRI, and Availability Pay is Y. The Work Start Time is 0800 and Work End Time is 1630. The 'AGENT WORK HOUR DETAILS' section includes fields for Investigation Totals (1), Excess Hours (27), Case Development (0), Scheduled Overtime (0), Available Hours (0), Credit Hours (0), Liasion (0), Excludable Days (2), Training Provided (0), Training Received (8), PT Training (6), Administrative (84), Leave (8), Others (0), and Total Hours (107). The 'INVESTIGATIONS' section has a table with columns for UID Number and Total Hours. The first row has UID Number (b)(7)(E) and Total Hours (1). The 'TOTAL UID HOURS' field is empty. An 'UPDATE' button is at the bottom right. The status bar shows 'Record: 1/1'.

Select the “Add Agent” icon again to add another record.

The screenshot shows the 'IDS INVESTIGATOR DESKTOP - [WTS_WINDOW]' application. The menu bar includes ACTION, QUERY, RECORD, HELP, EXIT, and Window. The toolbar contains icons for ADD AGENT TO PAY PERIOD, SAVE, PRINT, and EXIT. The 'ADD AGENT TO PAY PERIOD' icon is circled in red. Below the menu bar, there are fields for Agent Idno, Agent Office, Agent Series, Agent Grade, PPE Date, and BASIC HOURS. The Agent Last Name and Agent First Name fields are empty, and Agent MI is empty. The Work Start Day, Work End Day, and Availability Pay fields are empty. The Work Start Time and Work End Time fields are empty. The 'AGENT WORK HOUR DETAILS' section includes fields for Investigation Totals (0), Excess Hours (0), Case Development (0), Scheduled Overtime (0), Available Hours (0), Credit Hours (0), Liasion (0), Excludable Days (0), Training Provided (0), Training Received (0), PT Training (0), Administrative (0), Leave (0), Others (0), and Total Hours (0). The 'INVESTIGATIONS' section has a table with columns for UID Number and Total Hours. The 'TOTAL UID HOURS' field is empty. An 'UPDATE' button is at the bottom right. The status bar shows 'ADD AGENT TO PAY PERIOD' and 'Record: 1/1'.

Click the Exit button to quit. Answer “Yes” if you have already saved the record.

The screenshot shows the 'IDS INVESTIGATOR DESKTOP - [WTS_WINDOW]' interface. At the top, there is a menu bar with 'ACTION', 'QUERY', 'RECORD', 'HELP', 'EXIT', and 'Window'. Below the menu bar is a toolbar with icons for 'ESC', 'SAVE', a calculator, and a notepad. The 'EXIT' button, represented by a red square with a white 'X', is circled in red. The main area contains a form for agent information, including fields for Agent Office (04PR), Agent Series (1811), Agent Grade (14), PPE Date (20-NOV-1999), BASIC HOURS (80), Agent Last Name, Agent First Name, Agent MI, Work Start Day (MON), Work End Day (FRI), Availability Pay (Y), Work Start Time (0800), and Work End Time (1630). Below this is a section for 'AGENT WORK HOUR DETAILS' and 'INVESTIGATIONS'. The 'AGENT WORK HOUR DETAILS' section includes fields for Investigation Totals (1), Case Development (0), Available Hours (0), Liasion (0), Training Provided (0), Training Received (8), PT Training (6), Administrative (84), Leave (8), Others (0), and Total Hours (107). The 'INVESTIGATIONS' section includes a 'Forms' dialog box with a red background and a white 'X' icon, displaying the message 'Form will exit without saving, continue?' with 'YES' and 'NO' buttons. There is also an 'UPDATE' button at the bottom right of the 'INVESTIGATIONS' section. The bottom of the window has an 'EXIT' button.

To modify an existing record in WTS, click the Entry/Modify button on the Work Hour Tracking System screen.

The screenshot shows the 'IDS INVESTIGATOR DESKTOP' interface with the 'WORK HOUR TRACKING SYSTEM' screen. The menu bar includes 'Action' and 'Window'. The main area displays four buttons: 'Entry/Modify WTS' (circled in red), 'View WTS', 'Reports Menu', and 'Return to Main Menu'. Each button has a corresponding icon: a laptop for 'Entry/Modify WTS', a computer monitor for 'View WTS', a document with a magnifying glass for 'Reports Menu', and a blue arrow pointing left for 'Return to Main Menu'.

Select the file folder icon to modify an entry.

IDS INVESTIGATOR DESKTOP - [WTS_WINDOW]

ACTION QUERY RECORD HELP EXIT Window

PRINT ESC SAVE

MODIFY AGENT PAY PERIOD

Agent Idno Agent Office: Agent Series: Agent Grade: PPE Date: BASIC HOURS:

Agent Last Name: Agent First Name: Agent MI:

Work Start Day: Work End Day: Availability Pay:

Work Start Time: Work End Time:

AGENT WORK HOUR DETAILS

Investigation Totals: Excess Hours:

Case Development: Scheduled Overtime:

Available Hours: Credit Hours:

Liasion: Excludable Days:

Training Provided:

Training Received:

PT Training:

Administrative:

Leave:

Others:

Total Hours:

INVESTIGATIONS

UID Number	Total Hours
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>

TOTAL UID HOURS:

UPDATE

ADD AGENT TO PAY PERIOD

Record: 1/1

A list of records for the current fiscal quarter for your office will appear. (You cannot modify records from prior quarters.)

IDS INVESTIGATOR DESKTOP - [WTS_WINDOW]

ACTION QUERY RECORD HELP EXIT Window

PRINT ESC SAVE

SELECT AGENT FOR UPDATE

Click button next to Agent IDNO to insert WTS data sheet.

Agent #	Date	Last Name	First Name	MI	Office
<input type="checkbox"/>	13-JUL-2002				40MN
<input type="checkbox"/>	13-JUL-2002				03TD
<input type="checkbox"/>	13-JUL-2002				40CR
<input type="checkbox"/>	13-JUL-2002				60BT
<input type="checkbox"/>	27-JUL-2002				60BT
<input type="checkbox"/>	13-JUL-2002				60NF
<input type="checkbox"/>	27-JUL-2002				60NF
<input type="checkbox"/>	13-JUL-2002				10SY
<input type="checkbox"/>	26-JAN-2002				40SL
<input type="checkbox"/>	13-JUL-2002				40SL
<input type="checkbox"/>	13-JUL-2002				30PX
<input type="checkbox"/>	27-JUL-2002				30PX
<input type="checkbox"/>	13-JUL-2002				50ES
<input type="checkbox"/>	27-JUL-2002				50ES

CLOSE

Record: 1/433

<OSC> <DBG>

The previously entered record will appear. Make corrections, save, and exit.

[illegible]

To run reports, select the Reports button from the Welcome screen.

IDS INVESTIGATOR DESKTOP

ORACLE

Welcome

Investigative Data System Agents Manual

Workhour Tracking System Analysis

Physical Training Module Maintenance

Reports

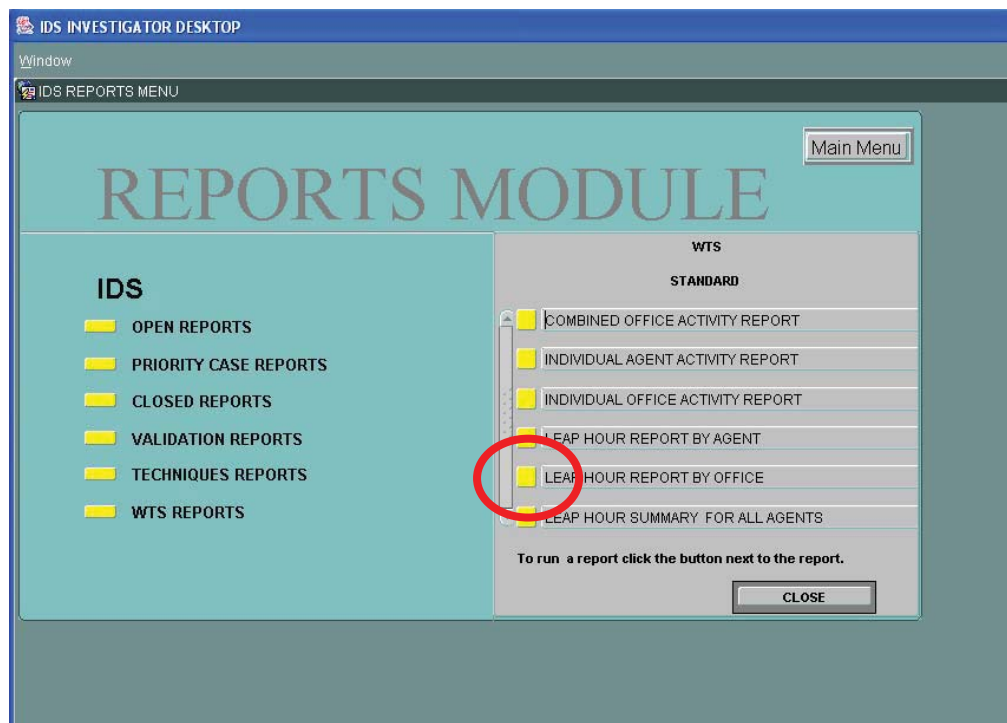
SYSTEM NOTE: The functions keys have been remapped for the following keys:
 F1 - Help, F7 - Enter Query, F8 - Execute Query, F9 - List Values, F10 - Save

IDS APPLICATIONS
 Record: 1/1

Select WTS Reports.



Select the desired report.



Add office and date parameters. Use % as the wildcard.

Report will appear on the screen.

Investigator Name	Grade	Avail Pay?	WrkDys In Per	Exclude Days	Adjust WrkDays	Excess Hrs Wrkd	Avg Daily Availability
Office: 04PR - INTERNAL OPERATIONS DIRECTORATE							
(b)(6), (b)(7)(C)	14	Y	160	44	116	266.50	2.297414
(b)(6), (b)(7)(C)	14	Y	160	26	134	320.50	2.391791
(b)(6), (b)(7)(C)	15	Y	160	61	99	254.00	2.565657
(b)(6), (b)(7)(C)	14	Y	160	41	119	281.00	2.361345
(b)(6), (b)(7)(C)	14	Y	160	52	108	323.00	2.990741
(b)(6), (b)(7)(C)	14	Y	160	41	119	269.50	2.264706
(b)(6), (b)(7)(C)	14	Y	160	35	125	461.00	3.688000
Office Totals:			1120	300	820	2175.5	2.653049
GRAND TOTALS:			1120	300	820	2175.5	2.653049

From the menu bar, select File | Print for a paper copy.

Adobe Reader - [112622060919064242.pdf]

File Edit View Document Tools Window Help

Create Adobe PDF Online...

Open... Ctrl+O

Save... Ctrl+S

Save as Text...

Document Properties... Ctrl+D

Print Setup... Shift+Ctrl+P

Print... Ctrl+P

Print to Internet Printing...

Exit Ctrl+Q

Page: 1

LEAP Hour Report for 04INT
2006/01/08 to 2006/09/16

Grade	Avail Pay?	WrkDys In Per	Exclude Days	Adjust WrkDays	Excess Hrs Wrkd	Avg Daily Availability
AL OPERATIONS DIRECTORATE						
14	Y	160	44	116	266.50	2.297414
14	Y	160	26	134	320.50	2.391791
15	Y	160	61	99	254.00	2.565657
14	Y	160	41	119	281.00	2.361345
14	Y	160	52	108	323.00	2.990741
14	Y	160	41	119	269.50	2.264706
14	Y	160	35	125	461.00	3.688000
Office Totals:		1120	300	820	2175.5	2.653049
GRAND TOTALS:		1120	300	820	2175.5	2.653049

Select your printer.

Adobe Reader - [112622060919062526.pdf]

File Edit View Document Tools Window Help

Save as Copy

Search

Select

Page: 1

2006/09/19

LEAP Hour Report for 04INT
2006/01/08 to 2006/09/16

Investigator Name

Office: 04PR - INTERNAL

Print

Printer: **HP LaserJet 5100 PCL 6**

Status: Ready

Print Range: ☒ All ☐ Current view ☐ Current page

Pages from 1 to 1

Subset: All pages in range ☐ Reverse pages

Page Handling: Copies: 1 ☐ Collate

Page Scaling: ☒ Reduce to Printer Margins ☐ Auto-Rotate and Center ☐ Choose Paper Source by PDF page size

☐ Print to file

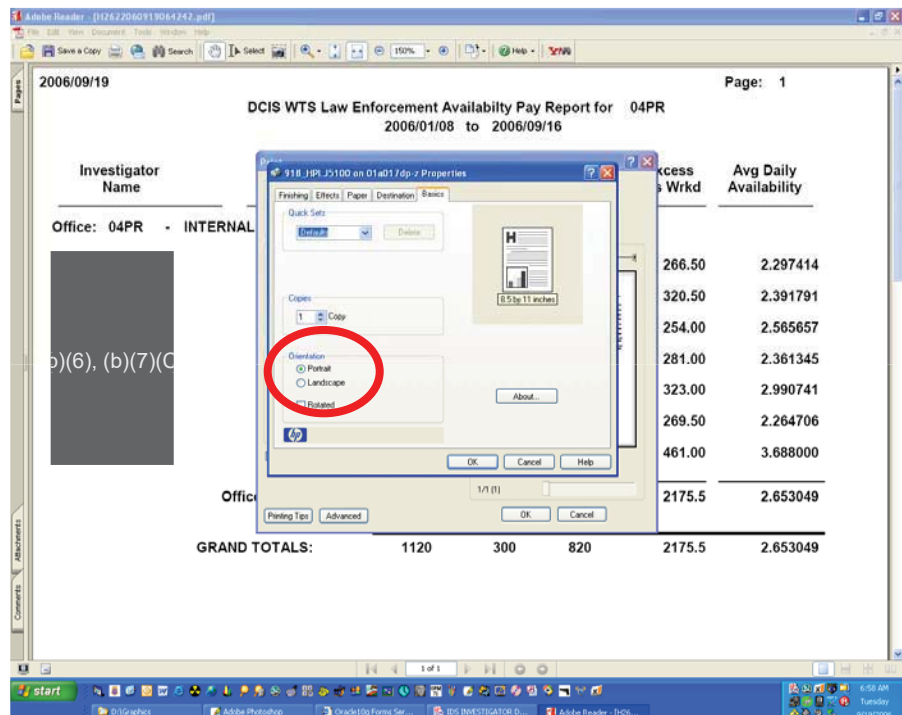
Printing Tips Advanced

OK Cancel

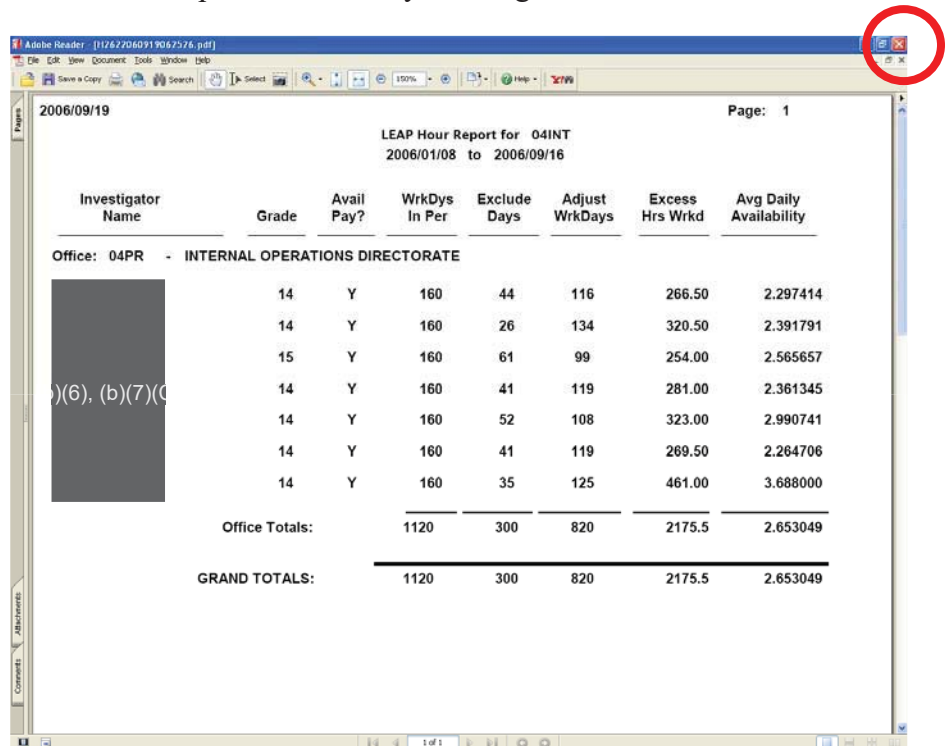
Excess Hrs Wrkd	Avg Daily Availability
266.50	2.297414
320.50	2.391791
254.00	2.565657
281.00	2.361345
323.00	2.990741
269.50	2.264706
461.00	3.688000
2175.5	2.653049

GRAND TOTALS: 1120 300 820 2175.5 2.653049

Click the properties button to ensure that report is set for landscape or portrait, as appropriate. Click OK.



After the report prints, close the report on screen by clicking the red X.



Click the “Main Menu” button in the upper right corner to close the reports menu and return to the main menu.



ATTACHMENT F

EXAMPLES OF EXCLUDABLE DAYS - TRAVEL TIME

1. Written Guidance

1.1. 5 USC 5545a(f)(1). “A criminal investigator who is eligible for availability pay shall receive such pay during any period such investigator is: attending agency sanctioned training; on agency approved sick leave or annual leave; on agency ordered travel status; or on excused absence with pay for relocation purposes.”

1.2. 5 CFR 550.183(b). “For the purpose of this section, *regular workday* means each day the criminal investigator’s basic workweek during which the investigator works at least 4 hours, excluding...hours during which an investigator is engaged in agency-approved training, is traveling under official travel orders, is on approved leave, or is on excused absence with pay (including paid holidays).” (Note that this definition includes military leave, where the statute does not.)

1.3. SAM 54.6.g.(17).(e). restricts travel on orders to those days in which the criminal investigator “was in transit on agency-ordered travel” for 4 or more hours.

2. Discussion

2.1. The statute uses the concept of excludable days—authorizing availability pay on days when the employee either is not working at all (leave, holidays, relocation) or is not working on normal job tasks (training and travel). The Office of Personnel Management’s (OPM’s) guidance in addressing the travel portion of the exemption adds the requirement for being under official travel orders. The intent of SAM Chapter 54 is to comply with OPM guidance while disallowing exclusion of days when the criminal investigator is working normal job tasks and is not in transit, even though on orders.

2.2. The “rule” behind these examples provides a “benefit” to criminal investigators when they travel 4 or more hours in a regular workday and work more than 4 hours the same day, as in example 3.4.; the day is excludable and any hours over 8 are also counted as excess hours.

3. Examples

3.1. A criminal investigator travels 2 hours Monday from the metro D.C. area to southern Virginia, conducts a 4-hour interview, and travels 2 hours back to the office. Even though the criminal investigator traveled 4 hours, the day is **not** excludable because no orders were issued for “local” area travel.

3.2. A criminal investigator travels 1 hour from the office in Chicago to interview a witness. After the interview, the criminal investigator gets stuck in a traffic jam for 2 hours. The criminal investigator returns to the office. In the afternoon, the criminal investigator spends an hour

driving to and from a Defense contractor to pick up subpoenaed records. Although the total time in traffic exceeds 4 hours for the day, the day is **not** excludable because no orders were issued for local area travel.

3.3. A criminal investigator travels 4 hours Tuesday from Atlanta to western Tennessee; meets with an Assistant U.S. Attorney (AUSA) for 2 hours and travels 4 hours back to Atlanta. Even though the criminal investigator traveled for more than 4 hours, the day is **not** excludable because no orders were issued for travel.

3.4. A criminal investigator has “single day orders” covering meals and incidentals only, travels 4 hours Tuesday from Atlanta to western Tennessee, meets with the AUSA for 4 hours, and travels 4 hours back to Atlanta. The day **is** excludable because travel was under orders. Single day orders are usually issued for travel of 12 hours or more without lodging. If orders are appropriate, exclusion of the day is permissible, as in this example.

3.5. A criminal investigator with orders travels 5 hours Wednesday from Phoenix to Las Vegas for a consensual monitoring, works 3 hours in Las Vegas and travels 5 hours back on Thursday, working 3 hours upon arrival to complete voucher and monitoring paperwork. **Both** days are excludable because travel was under orders and exceeded 4 hours each day.

NOTE: The statute and SAM guidance allow both days to be excludable. OPM guidance is less clear, as it combines “days” with “hours” in its definition. It defines the regular workday as a day during the basic workweek (this example), but excludes hours when the investigator is traveling under official orders (both days in this example). Counting both days as excludable enables DCIS to provide a consistent way of handling the travel exemption, and is consistent with the DCIS rule for part-days of leave or training, e.g., 4 hours firearms re-qualification plus 5 hours work = 1 excludable day and 1 excess hour.

3.6. A criminal investigator travels on orders Monday for 6 hours from Los Angeles to Hartford to participate in an inspection. The criminal investigator inspects Hartford on Tuesday, drives 2 hours to Boston on Wednesday, inspects Boston on Wednesday and Thursday, flies 3 hours to Philadelphia on Thursday, and flies 6 hours home to Los Angeles on Friday. Monday and Friday **are** excludable days because travel exceeded 4 hours and the criminal investigator was in transit on orders. Tuesday, Wednesday, and Thursday are **not** excludable because, although on orders, the criminal investigator was not in transit 4 or more hours those days.

3.7. A criminal investigator travels on orders Sunday from Denver to North Carolina to work on a terrorism task force. The criminal investigator works in North Carolina for 2 weeks and returns to Denver on the second Friday, flying 6 hours to and from Denver. The first Sunday is **not** excludable because Saturday and Sunday are not part of the criminal investigator’s basic workweek (statutory reason) and because the WTS LEAP computations already exclude Saturdays and Sundays (practical implementation reason). The travel time on the first Sunday counts as excess hours because the hours are associated with work. The second Friday **is**

excludable because transit time exceeds 4 hours. Monday through Friday the first week and Monday through Thursday the second week **are not** excludable while the criminal investigator is working under orders on the task force but is not in transit.



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

March 30, 2015

MEMORANDUM FOR DEFENSE CRIMINAL INVESTIGATIVE SERVICE EMPLOYEES

**SUBJECT: Interim Policy for Special Agents Manual Chapter 54, Law Enforcement
Availability Pay, Concerning Compensatory Time Off for Travel**

Effective April 5, 2015, this interim policy memorandum provides guidance on requesting compensatory time off for travel (CTOFT) for time spent in travel status. This memorandum supplements IGDINST 1422.1: Tours of Duty, Overtime, Time and Attendance Reporting, and applies to all Defense Criminal Investigative Service employees, **except** members of the Senior Executive Service.

Compensatory Time Off for Travel

Supervisors must track and manage compensatory time granted for time in a travel status separately from other forms of compensatory time off. If an employee is compensated for travel by overtime, compensatory time, or LEAP (i.e., the travel counted as hours of work or unscheduled duty hours for criminal investigators), then compensatory time off for travel is not authorized. For criminal investigators, time spent in a travel status that involves investigative or other operational activity (i.e., travel has a nexus to an investigation) is compensated by LEAP; therefore, in this instance they are ineligible for travel compensatory time. However, if criminal investigative personnel spend time in a travel status for training, conferences, policy meetings, or other travel that does not involve investigative or operational activity, they are eligible to earn compensatory time off for travel if it is not otherwise compensable.

When requesting CTOFT, DCIS employees should utilize the attached worksheet and DCIS Form 54, and refer to IGDINST 1422.1 Ch. 3, ¶ D, Crediting Compensatory Time for Travel, for guidance.

Additional Information

Direct questions to your Human Capital Advisory Services representative and your supervisor. If you have any questions related to this interim policy memorandum, please contact Program Director (b)(6), (b)(7)(C) Internal Operations Directorate at 703-699 (b)(6), (b)(7)

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

Assistant Inspector General
for Investigations

~~FOR OFFICIAL USE ONLY~~

Attachments:

1. Compensatory Time for Travel Worksheet for Non-Local Travel, SCMS
Rev.2.0/BQW_Exh62.doc
2. DCIS Form 54 (Example includes line item "S" to record Compensatory Time-Off Hours
being claimed)
3. OPM Fact Sheet: Compensatory Time Off for Travel

Compensatory Time for Travel Worksheet for Non-Local Travel

Employee Name: _____

Travel Dates for Comp Time: _____

Time Periods	Actual Time ¹	Net Time ²
Part I – Travel to TDY Station		
Travel from home* or office to terminal ³ <i>*Time spent traveling from home to a transportation terminal that is within 50 miles of the employee's official worksite is not creditable.</i>		
Time waiting at terminal ⁴		
Additional time due to delay or cancellation of scheduled flight/train (if applicable) ⁵		
Travel time from first terminal to the next one ⁶		
Time between flights/trains (if applicable) ⁷		
Travel time from second terminal to the next one (if applicable) ⁸		
Time at final terminal and travel from terminal to final destination ⁹		
Part II – Travel from TDY Station		
Travel from hotel or worksite to terminal and time waiting at terminal ¹⁰		
Additional time due to delay or cancellation of scheduled flight/train (if applicable) ¹¹		
Travel time from first terminal to the next one ¹²		
Time between flights/trains, if applicable ¹³		
Travel time from second terminal to the next one (if applicable) ¹⁴		
Time at final terminal ¹⁵		
Travel from terminal to final destination* ¹⁶ <i>*Time spent traveling from a transportation terminal that is within 50 miles of the employee's official worksite and their home is not creditable.</i>		
Total		

Reduce the total hours by:

- Time that overlaps regular duty hours.
- Personal time for rest, sleep, etc. during usual waiting period; any additional time beyond the usual waiting period of 2 hours for domestic or 3 hours for international flights.
- Regular commuting time for trips to and from the initial and final departure terminal and home.

Supervisor's signature/date*

*indicates earned comp time for travel was reviewed and approved.

(Front)

Footnotes

-
- ¹ Record the local time in 15-minute increments; times should be the same as the times used for completing the associated travel voucher.
- ² Record the net (elapsed) creditable time after any adjustments, recorded in 15-minute increments.
- ³ Reduce time by the amount for employee's regular commute time to his/her office (which is _____) and by the amount that overlaps regular duty hours.
- ⁴ Actual time at terminal (not to exceed 2 hours); this includes time waiting in line to check in but not in the parking lot or traveling from the parking lot to the terminal; reduce time by the amount that overlaps regular duty hours.
- ⁵ Reduce time by the amount that overlaps regular duty hours.
- ⁶ Reduce time by the amount that overlaps regular duty hours
- ⁷ Actual time at terminal (not to exceed 2 hours); reduce time by the amount that overlaps regular duty hours; if flight/train is cancelled, waiting time may be credited up to the time that the employee is notified or becomes aware of the cancellation (time of notification: _____); travel time to and from a hotel may be credited for an overnight stay.
- ⁸ Reduce time by the amount that overlaps regular duty hours; when more than one intervening stop is involved, insert additional rows below this one.
- ⁹ For picking up baggage, making transportation arrangements, and travel time to the hotel or work site, reduce time by the amount that overlaps regular duty hours.
- ¹⁰ Actual time at terminal (not to exceed 2 hours); reduce time by the amount that overlaps regular duty hours.
- ¹¹ Reduce time by the amount that overlaps regular duty hours
- ¹² Reduce time by the amount that overlaps regular duty hours
- ¹³ Reduce time by the amount that overlaps regular duty hours; if flight/train is cancelled, waiting time may be credited up to the time that the employee is notified or becomes aware of the cancellation (time of notification: _____); travel time to and from a hotel may be credited for an overnight stay.
- ¹⁴ When more than one intervening stop is involved, insert additional rows below this one which duplicate periods four and five.
- ¹⁵ For picking up baggage and making transportation arrangements, reduce time by the amount that overlaps normal duty hours.
- ¹⁶ Reduce time by the amount for employee's normal commute time from his/her office to home that overlaps normal duty hours.

(Back)

BIWEEKLY ACTIVITY REPORT (Special Agents)		Name (Last, First, MI)										Grade:		ID #:		
Reporting Period From: To:					Office:					Availability Pay: (X) Yes () No						
BASIC WORK WEEK DAYS					From: Monday To: Friday		HOURS					Position: () HQ () Field Mgr () Agent				
ACTIVITIES		TOTALS	1/0/1900 SUN	1/1/1900 MON	1/2/1900 TUE	1/3/1900 WED	1/4/1900 THU	1/5/1900 FRI	1/6/1900 SAT	1/7/1900 SUN	1/8/1900 MON	1/9/1900 TUE	1/10/1900 WED	1/11/1900 THU	1/12/1900 FRI	1/13/1900 SAT
	Time In															
	Time Out															
	Time In															
A. Investigations UID	Time Out															
TOTALS FROM - PAGE 3 -----																
B. Case Development																
C. Availability Hours																
E. Liaison																
G. Training (received or provided)																
I. Physical Fitness Training																
J. Administration																
K. Leave																
L. All Other (holidays, comp/credit hrs taken)																
M. Total Hours																
N. Excess Over Basic Hrs (LEAP agents only)																
O. Scheduled Overtime																
P. Credit Hours Worked (No LEAP agents)																
Q. Excludable Days (LEAP agents only)																
R. Telecommute Days (Mark with "TW")																
S. Compensatory Time-Off for Travel																
								Remarks:								
Employee Signature & Date								Supervisor Signature & Date								

U.S. OFFICE OF PERSONNEL MANAGEMENT

PAY & LEAVE PAY ADMINISTRATION

Fact Sheet: Compensatory Time Off for Travel

Description

Compensatory time off for travel is earned by an employee for time spent in a travel status away from the employee's official duty station when such time is not otherwise compensable.

Employee Coverage

Compensatory time off for travel may be earned by an "employee" as defined in 5 U.S.C. 5541(2) who is employed in an "Executive agency" as defined in 5 U.S.C. 105, without regard to whether the employee is exempt from or covered by the overtime pay provisions of the Fair Labor Standards Act of 1938, as amended. For example, this includes employees in senior-level (SL) and scientific or professional (ST) positions, but not members of the Senior Executive Service or Senior Foreign Service or Foreign Service officers. Effective April 27, 2008, prevailing rate (wage) employees are covered under the compensatory time off for travel provision. See CPM 2008-04.)

"Compensable"

Compensatory time off for travel may only be earned for time in a travel status when such time is not otherwise "compensable." Compensable refers to periods of time creditable as hours of work for the purpose of determining a specific pay entitlement. For example, certain travel time may be creditable as hours of work under the overtime pay provisions in 5 CFR 550.112(g) or 551.422. (See fact sheet on hours of work for travel.)

Creditable Travel

To be creditable under this provision, travel must be officially authorized. In other words, travel must be for work purposes and must be approved by an authorized agency official or otherwise authorized under established agency policies.

For the purpose of compensatory time off for travel, time in a travel status includes-

- Time spent traveling between the official duty station and a temporary duty station;
- Time spent traveling between two temporary duty stations; and
- The "usual waiting time" preceding or interrupting such travel (e.g., waiting at an airport or train station prior to departure). The employing agency has the sole and exclusive discretion to determine what is creditable as "usual waiting time." An "extended" waiting period-i.e., an unusually long wait during which the employee is free to rest, sleep, or otherwise use the time for his or her own purposes-is not considered time in a travel status.

Commuting Time

- Travel outside of regular working hours between an employee's home and a temporary duty station or transportation terminal outside the limits of his or her official duty station is considered creditable travel time. However, the agency must deduct the employee's normal home-to-work/work-to-home commuting time from the creditable travel time.
- Travel outside of regular working hours between a worksite and a transportation terminal is creditable travel time, and no commuting time offset applies.
- Travel outside of regular working hours to or from a transportation terminal within the limits of the employee's official duty station is considered equivalent to commuting time and is not creditable travel time.

Crediting and Use

Compensatory time off for travel is credited and used in increments of one-tenth of an hour (6 minutes) or one-quarter of an hour (15 minutes). Employees must comply with their agency's procedures for requesting credit within the time period required by the agency. Employees must also comply with their agency's policies and procedures for scheduling and using earned compensatory time off for travel.

Forfeiture

Compensatory time off for travel is forfeited-

- If not used by the end of the 26th pay period after the pay period during which it was earned. (See Notes 1 and 2.)
- Upon voluntary transfer to another agency;
- Upon movement to a noncovered position; or
- Upon separation from the Federal Government. (See Note 1.)

Under no circumstances may an employee receive payment for unused compensatory time off for travel.

Note 1: See exceptions for uniformed service or an on-the-job injury with entitlement to injury compensation at 5 CFR 550.1407(a)(2) and Question 24 of the Questions and Answers on Compensatory Time Off for Travel (under References below).

Note 2: See exception due to an exigency of the service beyond the employee's control at 5 CFR 550.1407(e) and Question 25 of the Questions and Answers on Compensatory Time Off for Travel (under References below).

Limitations

Compensatory time off for travel may not be considered in applying the biweekly or annual premium pay caps or the aggregate limitation on pay. There is no limitation on the amount of compensatory time off for travel an employee may earn.

References

- 5 U.S.C. 5550b
- 5 CFR 550, subpart N
- Questions and Answers on Compensatory Time Off for Travel (see Attachment 1 to CPM 2005-03)
- Examples of creditable travel time (see Attachment 2 to CPM 2005-03)
- Hours of Work for Travel

[Back to Top](#)

[Click here to skip navigation](#)

This website uses features which update page content based on user actions. If you are using assistive technology to view web content, please ensure your settings allow for the page content to update after initial load (this is sometimes called "forms mode"). Additionally, if you are using assistive technology and would like to be notified of items via alert boxes, please [follow this link to enable](#) alert boxes for your session profile.



Search...

GO

[Main](#)[About The Council](#)[Events](#)[Members](#)[News](#)[Transmittals](#)

01/27/2005
CPM 2005-03



Office of the Director

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

From:

KAY COLES JAMES
Director


Subject:

Compensatory Time Off for Travel

Download

Memo:

 (4.20 mb)

Section 203 of the Federal Workforce Flexibility Act of 2004 (Public Law 108-411, October 30, 2004) authorized a new form of compensatory time off for time spent by an employee in a travel status away from the employee's official duty station when such time is not otherwise compensable. (See [CPM 2004-22](#), November 1, 2004). The Office of Personnel Management (OPM) recently issued interim regulations implementing this new provision ([copy attached](#) ).

Effective Date

The regulations implementing the new form of compensatory time off for time in a travel status are effective on January 28, 2005. Agencies must credit covered employees who perform officially authorized travel on or after the effective date with any compensatory time off for time in a travel status to which they are entitled under the regulations. If an employee is on an extended period of officially authorized travel on the effective date, only the qualifying travel hours

occurring on or after the effective date are creditable for the purpose of earning the new compensatory time off.

Guidance

To assist agencies in implementing and administering this new provision, we are providing the attached questions and answers ([Attachment 1](#)) and some examples ([Attachment 2](#)) which illustrate how much compensatory time off an employee is entitled to earn for time spent in a travel status.

Additional Information

For additional information, agency Chief Human Capital Officers and/or Human Resources Directors should contact their assigned OPM Human Capital Officer. Employees should contact their agency human resources office for assistance.

cc: Chief Human Capital Officers
Human Resources Directors


[Attachment 1](#)

[Attachment 2](#)

www.opm.gov

Our Mission is to Recruit, Retain and Honor a World-Class
Workforce to Serve the American People.

www.usajobs.gov

[Accessibility](#) | [Privacy Policy](#) | [Contact Us](#) | [OPM.gov](#) | [USA.gov](#) | [Other Councils](#) | [PDF Help](#) 
Official website of the U.S. Government operated by the Office of Personnel Management

You have reached a collection of archived material.

The content available is no longer being updated and may no longer be applicable as a result of changes in law, regulation and/or administration. If you wish to see the latest content, please visit the [current version of the site](#).

Archived Content.

You have reached a collection of archive material. The content available is no longer being updated and may no longer be applicable as a result of changes in law, regulation and/or administration. If you wish to see the latest content, please visit the [current version of the site](#).

U.S. OFFICE OF PERSONNEL MANAGEMENT

[WWW.OPM.GOV](http://www.opm.gov)

Questions and Answers on Compensatory Time Off for Travel

Updated April 17, 2007

Q1. What is compensatory time off for travel?

A. Compensatory time off for travel is a separate form of compensatory time off that may be earned by an employee for time spent in a travel status away from the employee's official duty station when such time is not otherwise compensable.

Q2. Are all employees covered by this provision?

A. The compensatory time off provision applies to an "employee" as defined in 5 U.S.C. 5541(2) who is employed in an "Executive agency" as defined in 5 U.S.C. 105, without regard to whether the employee is exempt from or covered by the overtime pay provisions of the Fair Labor Standards Act of 1938, as amended. For example, this includes employees in senior-level (SL) and scientific or professional (ST) positions, but not members of the Senior Executive Service or Senior Foreign Service or Foreign Service officers. Effective April 27, 2008, prevailing rate (wage) employees are covered under the compensatory time off for travel provision.

(See [CPM 2008-04](#).)

Q3. Are intermittent employees eligible to earn compensatory time off for travel?

A. No. Compensatory time off for travel may be used by an employee when the employee is granted time

off from his or her scheduled tour of duty established for leave purposes. (See 5 CFR 550.1406(b).) Also see the definition of "scheduled tour of duty for leave purposes" in 5 CFR 550.1403. Employees who are on intermittent work schedules are not eligible to earn and use compensatory time off for travel because they do not have a scheduled tour of duty for leave purposes.

Q4. What qualifies as travel for the purpose of this provision?

A. To qualify for this purpose, travel must be officially authorized. In other words, travel must be for work purposes and must be approved by an authorized agency official or otherwise authorized under established agency policies. (Also see Q5.)

Q5. May an employee earn compensatory time off when he or she travels in conjunction with the performance of union representational duties?

A. No. The term "travel" is defined at 5 CFR 550.1403 to mean officially authorized travel—i.e., travel for work purposes approved by an authorized agency official or otherwise authorized under established agency policies. The definition specifically excludes time spent traveling in connection with union activities. The term "travel for work purposes" is intended to mean travel for agency-related work purposes. Thus, employees who travel in connection with union activities are not entitled to earn compensatory time off for travel because they are traveling for the benefit of the union, and not for agency-related work purposes.

Q6. An employee receives compensatory time off for travel only for those hours spent in a travel status. What qualifies as time in a travel status?

A. Travel status includes only the time actually spent traveling between the official duty station and a temporary duty station, or between two temporary duty stations, and the usual waiting time that precedes or interrupts such travel.

Q7. Is travel in connection with a permanent change of station (PCS) creditable for compensatory time off for travel?

A. Although PCS travel is officially authorized travel, it is not travel between an official duty station and a temporary duty station or between two temporary duty stations. Therefore, it is not considered time in a travel status for the purpose of earning compensatory time off for travel.

Q8. What is meant by "usual waiting time"?

A. Airline travelers generally are required to arrive at the airport at a designated pre-departure time (e.g., 1 or 2 hours before the scheduled departure, depending on whether the flight is domestic or international). Such waiting time at the airport is considered usual waiting time and is creditable time in a travel status. In addition, time spent at an intervening airport waiting for a connecting flight (e.g., 1 or 2 hours) also is creditable time in a travel status. In all cases, determinations regarding what is creditable as "usual waiting time" are within the sole and exclusive discretion of the employing agency.

Q9. What if an employee experiences an "extended" waiting period?

A. If an employee experiences an unusually long wait prior to his or her initial departure or between actual periods of travel during which the employee is free to rest, sleep, or otherwise use the time for his or her own purposes, the extended waiting time outside the employee's regular working hours is not creditable time in a travel status. An extended waiting period that occurs during an employee's regular working hours is compensable as part of the employee's regularly scheduled administrative workweek.

Q10. Do meal periods count as time in a travel status?

A. Meal periods during actual travel time or waiting time are not specifically excluded from creditable time in a travel status for the purpose of earning compensatory time off for travel. However, determinations regarding what is creditable as "usual waiting time" are within the sole and exclusive discretion of the employing agency.

Q11. What happens once an employee reaches a temporary duty station?

A. Time spent at a temporary duty station between arrival and departure is not creditable travel time for the purpose of earning compensatory time off for travel. Time in a travel status ends when the employee arrives at the temporary duty worksite or his or her lodging in the temporary duty station, wherever the employee arrives first. Time in a travel status resumes when an employee departs from the temporary duty worksite or his or her lodging in the temporary duty station, wherever the employee departs last.

Q12. When is it appropriate for an agency to offset creditable time in a travel status by the amount of time the employee spends in normal commuting between home and work?

A. If an employee travels directly between his or her home and a temporary duty station outside the limits of the employee's official duty station (e.g., driving to and from a 3-day conference), the agency must deduct the employee's normal home-to-work/work-to-home commuting time from the creditable travel time. The agency must also deduct an employee's normal commuting time from the creditable travel time if the employee is required—outside of regular working hours—to travel between home and a transportation terminal (e.g., an airport or train station) outside the limits of the employee's official duty station.

Q13. What if an employee travels to a transportation terminal within the limits of his or her official duty station?

A. An employee's time spent traveling outside of regular working hours to or from a transportation terminal within the limits of his or her official duty station is considered equivalent to commuting time and is not creditable time in a travel status for the purpose of earning compensatory time off for travel.

Q14. What if an employee travels from a worksite to a transportation terminal?

A. If an employee travels between a worksite and a transportation terminal, the travel time outside regular working hours is creditable as time in a travel status, and no commuting time offset applies. For example, after completing his or her workday, an employee may travel directly from the regular worksite to an airport to attend an out-of-town meeting the following morning. The travel time between the regular worksite and the airport is creditable as time in a travel status.

Q15. What if an employee elects to travel at a time other than the time selected by the agency?

A. When an employee travels at a time other than the time selected by the agency, the agency must determine the estimated amount of time in a travel status the employee would have had if the employee had traveled at the time selected by the agency. The agency must credit the employee with the lesser of (1) the estimated time in a travel status the employee would have had if the employee had traveled at the time selected by the agency, or (2) the employee's actual time in a travel status at a time other than that selected by the agency.

Q16. How is an employee's travel time calculated for the purpose of earning compensatory time off for travel when the travel involves two or more time zones?

A. When an employee's travel involves two or more time zones, the time zone from point of first departure must be used to determine how many hours the employee actually spent in a travel status for the purpose of accruing compensatory time off for travel. For example, if an employee travels from his official duty station in Washington, DC, to a temporary duty station in San Francisco, CA, the Washington, DC, time zone must be used to determine how many hours the employee spent in a travel status. However, on the return trip to Washington, DC, the time zone from San Francisco, CA, must be used to calculate how many hours the employee spent in a travel status.

Q17. How is compensatory time off for travel earned and credited?

A. Compensatory time off for travel is earned for qualifying time in a travel status. Agencies may authorize credit in increments of one-tenth of an hour (6 minutes) or one-quarter of an hour (15 minutes). Agencies must track and manage compensatory time off for travel separately from other forms of compensatory time off.

Q18. Is there a limitation on the amount of compensatory time off for travel an employee may earn?

A. No.

Q19. How does an employee request credit for compensatory time off for travel?

A. Agencies may establish procedures for requesting credit for compensatory time off for travel. An employee must comply with his or her agency's procedures for requesting credit of compensatory time off, and the employee must file a request for such credit within the time period established by the agency. An employee's request for credit of compensatory time off for travel may be denied if the request is not filed within the time period required by the agency.

Q20. Is there a form employees must fill out for requests to earn or use compensatory time off for travel?

A. There is not a Governmentwide form used for requests to earn or use compensatory time off for travel. However, an agency may choose to develop a form as part of its internal policies and procedures.

Q21. How does an employee use accrued compensatory time off for travel?

A. An employee must request permission from his or her supervisor to schedule the use of his or her accrued compensatory time off for travel in accordance with agency policies and procedures.

Compensatory time off for travel may be used when the employee is granted time off from his or her scheduled tour of duty established for leave purposes. Employees must use accrued compensatory time off for travel in increments of one-tenth of an hour (6 minutes) or one-quarter of an hour (15 minutes).

Q22. In what order should agencies charge compensatory time off for travel?

A. Agencies must charge compensatory time off for travel in the chronological order in which it was earned, with compensatory time off for travel earned first being charged first.

Q23. How long does an employee have to use accrued compensatory time off for travel?

A. An employee must use his or her accrued compensatory time off for travel by the end of the 26th pay period after the pay period during which it was earned or the employee must forfeit such compensatory time off, except in certain circumstances. (See Q24 and Q25 for exceptions.)

Q24. What if an employee is unable to use his or her accrued compensatory time off for travel because of uniformed service or an on-the-job injury with entitlement to injury compensation?

A. Unused compensatory time off for travel will be held in abeyance for an employee who separates, or is placed in a leave without pay status, and later returns following (1) separation or leave without pay to perform service in the uniformed services (as defined in 38 U.S.C. 4303 and 5 CFR 353.102) and a return to service through the exercise of a reemployment right or (2) separation or leave without pay due to an on-the-job injury with entitlement to injury compensation under 5 U.S.C. chapter 81. The employee must use all of the compensatory time off for travel held in abeyance by the end of the 26th pay period following the pay period in which the employee returns to duty, or such compensatory time off for travel will be forfeited.

Q25. What if an employee is unable to use his or her accrued compensatory time off for travel because of an exigency of the service beyond the employee's control?

A. If an employee fails to use his or her accrued compensatory time off for travel before the end of the 26th pay period after the pay period during which it was earned due to an exigency of the service beyond the employee's control, the head of an agency, at his or her sole and exclusive discretion, may extend the time limit for up to an additional 26 pay periods.

Q26. May unused compensatory time off for travel be restored if an employee does not use it by the end of the 26th pay period after the pay period during which it was earned?

A. Except in certain circumstances (see Q24 and Q25), any compensatory time off for travel not used by the end of the 26th pay period after the pay period during which it was earned must be forfeited.

Q27. What happens to an employee's unused compensatory time off for travel upon separation from Federal service?

A. Except in certain circumstances (see Q24), an employee must forfeit all unused compensatory time off for travel upon separation from Federal service.

Q28. May an employee receive a lump-sum payment for accrued compensatory time off for travel upon separation from an agency?

A. No. The law prohibits payment for unused compensatory time off for travel under any circumstances.

Q29. What happens to an employee's accrued compensatory time off for travel upon transfer to another agency?

A. When an employee voluntarily transfers to another agency (including a promotion or change to lower grade action), the employee must forfeit all of his or her unused compensatory time off for travel.

Q30. What happens to an employee's accrued compensatory time off for travel when the employee moves to a position that is not covered by the regulations in 5 CFR part 550, subpart N?

A. When an employee moves to a position in an agency not covered by the compensatory time off for travel provisions (e.g., the United States Postal Service), the employee must forfeit all of his or her unused compensatory time off for travel. However, the gaining agency may use its own legal authority to give the employee credit for such compensatory time off.

Q31. Is compensatory time off for travel considered in applying the premium pay and aggregate pay caps?

A. No. Compensatory time off for travel may not be considered in applying the biweekly or annual premium pay limitations established under 5 U.S.C. 5547 or the aggregate limitation on pay established under 5 U.S.C. 5307.

Q32. When are criminal investigators who receive availability pay precluded from earning compensatory time off for travel?

A. Compensatory time off for travel is earned only for hours not otherwise compensable. The term "compensable" is defined at 5 CFR 550.1403 to include any hours of a type creditable under other compensation provisions, even if there are compensation caps limiting the payment of premium pay for those hours (e.g., the 25 percent cap on availability pay and the biweekly premium pay cap). For availability pay recipients, this means hours of travel are not creditable as time in a travel status for compensatory time off purposes if the hours are (1) compensated by basic pay, (2) regularly scheduled overtime hours creditable under 5 U.S.C. 5542, or (3) "unscheduled duty hours" as described in 5 CFR 550.182(a), (c), and (d).

Q33. What constitutes "unscheduled duty hours" as described in 5 CFR 550.182(a), (c),

and (d)?

A. Under the availability pay regulations, unscheduled duty hours include (1) all irregular overtime hours—i.e., overtime work not scheduled in advance of the employee's administrative workweek, (2) the first 2 overtime hours on any day containing part of the employee's basic 40-hour workweek, without regard to whether the hours are unscheduled or regularly scheduled, and (3) any approved nonwork availability hours. However, special agents in the Diplomatic Security Service of the Department of State may count only hours actually worked as unscheduled duty hours.

Q34. Why are criminal investigators who receive availability pay precluded from earning compensatory time off when they travel during unscheduled duty hours?

A. The purpose of availability pay is to ensure the availability of criminal investigators (and certain similar law enforcement employees) for unscheduled duty in excess of a 40-hour workweek based on the needs of the employing agency. Availability pay compensates an employee for all unscheduled duty hours. Compensatory time off for travel is earned only for hours not otherwise compensable. Thus, availability pay recipients may not earn compensatory time off for travel during unscheduled duty hours because the employees are entitled to availability pay for those hours.

Q35. When is it possible for criminal investigators who receive availability pay to earn compensatory time off for travel?

A. When an employee who receives availability pay is required to travel on a non-workday or on a regular workday (during hours that exceed the employee's basic 8-hour workday), and the travel does not meet one of the four criteria in 5 U.S.C. 5542(b)(2)(B) and 5 CFR 550.112(g)(2), the travel time is not compensable as overtime hours of work under regular overtime or availability pay. Thus, the employee may earn compensatory time off for such travel, subject to the exclusion specified in 5 CFR 550.1404(b)(2) and the requirements in 5 CFR 550.1404(c),(d), and (e).

Under the provisions in 5 U.S.C. 5542(b)(2)(B) and 5 CFR 550.112(g)(2), travel time is compensable as overtime hours of work if the travel is away from the employee's official duty station and—

- (i) involves the performance of work while traveling,
- (ii) is incident to travel that involves the performance of work while traveling,
- (iii) is carried out under arduous conditions, or
- (iv) results from an event which could not be scheduled or controlled administratively.

The phrase "an event which could not be scheduled or controlled administratively" refers to the ability of an agency in the Executive Branch of the United States Government to control the scheduling of an event which necessitates an employee's travel. If the employing agency or another Executive Branch agency has any control over the scheduling of the event, including by means of approval of a contract for it, then the event is administratively controllable, and the travel to and from the event cannot be credited as overtime hours of work.

For example, an interagency conference sponsored by the Department of Justice would be considered a joint endeavor of the participating Executive Branch agencies and within their administrative control.

Under these circumstances, the travel time outside an employee's regular working hours is not compensable as overtime hours of work under regular overtime or availability pay. Therefore, the employee may earn compensatory time off for such travel, subject to the exclusion specified in 5 CFR 550.1404(b)(2) and the requirements in 5 CFR 550.1404(c), (d), and (e).

Q36. If an employee is required to travel on a Federal holiday (or an "in lieu of" holiday), is the employee entitled to receive compensatory time off for travel?

A. Although most employees do not receive holiday premium pay for time spent traveling on a holiday (or an "in lieu of" holiday), an employee continues to be entitled to pay for the holiday in the same manner as if the travel were not required. Thus, an employee may not earn compensatory time off for travel during basic (non-overtime) holiday hours because the employee is entitled to his or her rate of basic pay for those hours. Compensatory time off for travel may be earned by an employee only for time spent in a travel status away from the employee's official duty station when such time is not otherwise compensable.

Q37. If an employee's regularly scheduled tour of duty is Sunday through Thursday and the employee is required to travel on a Sunday during regular working hours, is the employee entitled to earn compensatory time off for travel?

A. No. Compensatory time off for travel may be earned by an employee only for time spent in a travel status away from the employee's official duty station when such time is not otherwise compensable. Thus, an employee may not earn compensatory time off for travel for traveling on a workday during regular working hours because the employee is receiving his or her rate of basic pay for those hours.

Q38. May an agency change an employee's work schedule for travel purposes?

A. An agency may not adjust the regularly scheduled administrative workweek that normally applies to an employee (part-time or full-time) solely for the purpose of including planned travel time not otherwise considered compensable hours of work. However, an employee is entitled to earn compensatory time off for travel for time spent in a travel status when such time is not otherwise compensable.

Q39. Is time spent traveling creditable as credit hours for an employee who is authorized to earn credit hours under an alternative work schedule?

A. Credit hours are hours an employee elects to work, with supervisory approval, in excess of the employee's basic work requirement under a flexible work schedule. Under certain conditions, an agency may permit an employee to earn credit hours by performing productive and essential work while in a travel status. See OPM's Handbook on Alternative Work Schedules at http://www.opm.gov/oca/worksch/HTML/Cred_hrs.htm#travel for the conditions that must be met. If those conditions are met and the employee does earn credit hours for travel, the time spent traveling would be compensable and the employee would not be eligible to earn compensatory time off for travel. If the conditions are not met, the employee would be eligible to earn compensatory time off for travel.

Q40. May an agency restore an employee's forfeited "use-or-lose" annual leave because

the employee elected to use earned compensatory time off for travel instead of using his or her excess annual leave?

A. Section 6304(d) of title 5, United States Code, prescribes the conditions under which an employee's forfeited annual leave may be restored to an employee. (See fact sheet on restored annual leave at <http://www.opm.gov/oca/leave/HTML/RESTORE.asp>.) There is no legal authority to restore an employee's forfeited annual leave because the employee elected to use earned compensatory time off for travel instead of using his or her excess annual leave.

Q41. If an employee is eligible to receive overtime pay for a period of travel because the travel meets one of the four criteria in 5 CFR 550.112(g)(2), is the employee eligible to earn compensatory time off for travel for any portion of the travel which may not be compensable because of the biweekly cap on premium pay?

A. No. Compensatory time off for travel may be earned by an employee only for time spent in a travel status away from the employee's official duty station when such time is not otherwise compensable. The term "compensable" is defined at 5 CFR 550.1403 to make clear what periods of time are "not otherwise compensable" and thus potentially creditable for the purpose of earning compensatory time off for travel. Time is considered compensable if the time is creditable as hours of work for the purpose of determining a specific pay entitlement (e.g., overtime pay for travel meeting one of the four criteria in 5 CFR 550.112(g)(2)) even when the time may not actually generate additional compensation because of applicable pay limitations (e.g., biweekly premium pay cap). The capped premium pay is considered complete compensation for all hours of work creditable under the premium pay provisions.

In other words, even though an employee may not receive overtime pay for all of his or her travel hours because of the biweekly premium pay cap, all of the travel time is still considered to be compensable under 5 CFR 550.112(g)(2). Under these circumstances, the employee has been compensated fully under the law for all of the travel hours and the employee may not earn compensatory time off for any portion of such travel not generating additional compensation because of the biweekly cap on premium pay.

Q42. May an employee who receives administratively uncontrollable overtime (AUO) pay under 5 U.S.C. 5545(c)(2) earn compensatory time off for travel?

A. If such employee's travel time is not compensable under 5 CFR 550.112(g) or 5 CFR 551.422, as applicable, and meets the requirements in 5 CFR part 550, subpart N, the employee is eligible to earn compensatory time off for travel for time spent in a travel status.

Q43. If a part-time employee's regularly scheduled tour of duty is Monday through Friday, 8:00 a.m. to 2:30 p.m., and the employee is required to travel on a Friday from 2:30 p.m. to 4:30 p.m., is the employee entitled to earn compensatory time off for travel for those 2 hours?

A. It depends. If the travel qualifies as compensable hours of work under 5 U.S.C. 5542(b)(2)(B) and 5 CFR 550.112(g)(2)—i.e., the travel involves or is incident to the performance of actual work, is carried out under arduous and unusual conditions, or results from an event which could not be scheduled or

controlled administratively—the employee may not be credited with compensatory time off for travel hours. (Such travel time outside a part-time employee's scheduled tour of duty, but not in excess of 8 hours in a day or 40 hours in a week, would be non-overtime hours of work compensated at the employee's rate of basic pay.) If the travel time does not qualify as compensable hours of work and meets the other requirements in 5 CFR part 550, subpart N, the part-time employee would be entitled to earn compensatory time off for those 2 hours. We note travel time is always compensable hours of work if it falls within an employee's regularly scheduled administrative workweek. (See 5 U.S.C. 5542(b)(2)(A) and 5 CFR 550.112(g)(1).) For a part-time employee, the regularly scheduled administrative workweek is defined in 5 CFR 550.103 as the officially prescribed days and hours within an administrative workweek during which the employee was scheduled to work in advance of the workweek. An agency may not adjust the regularly scheduled administrative workweek normally applied to an employee (part-time or full-time) solely for the purpose of including planned travel time otherwise not considered compensable hours of work.

Q44. Does an upgrade in travel accommodations impact an employee's entitlement to compensatory time off for travel?

A. Allowing an employee to upgrade his or her travel accommodations (e.g., to business class) does not eliminate his or her eligibility to earn compensatory time off for travel.

 [Back to top](#)

[Return to Compensation Memoranda Main Page](#)

This page can be found on the web at the following url: <http://archive.opm.gov/oca/compmemo/2005/2005-03-att1.asp>

U.S. Office of Personnel Management

1900 E Street, NW, Washington, DC 20415 | (202) 606-1800 | TTY (202) 606-2532

You have reached a collection of archived material.

The content available is no longer being updated and may no longer be applicable as a result of changes in law, regulation and/or administration. If you wish to see the latest content, please visit the [current version of the site](#).

Archived Content.

You have reached a collection of archive material. The content available is no longer being updated and may no longer be applicable as a result of changes in law, regulation and/or administration. If you wish to see the latest content, please visit the [current version of the site](#).

U.S. OFFICE OF PERSONNEL MANAGEMENT

WWW.OPM.GOV

Compensatory Time Off for Travel:

Updated April 17, 2007

Examples of Creditable Travel Time

Example 1: Travel to a temporary duty station on a workday

From home to business meeting

6:00 - 7:00 a.m.	7:00 - 8:00 a.m.	8:00 - 8:30 a.m.	8:30 - 11:30 a.m.	11:30 a.m. - 12:30 p.m.
Drive to airport	Wait at airport	Wait at airport	Plane departs/lands	Drive to worksite
<i>Noncreditable travel time</i>	<i>Creditable travel time</i>	<i>Regular working hours</i>	<i>Regular working hours</i>	<i>Regular working hours</i>

From business meeting to home

4:30 - 5:30 p.m.	5:30 - 7:00 p.m.	7:00 - 10:00 p.m.	10:00 - 11:00 p.m.
Drive to airport	Wait at airport	Plane departs/lands	Drive home
<i>Creditable travel time</i>	<i>Creditable travel time</i>	<i>Creditable travel time</i>	<i>Noncreditable travel time</i>

On a workday, an employee is required to travel from home to a temporary duty station for an afternoon meeting. The employee's regular working hours are 8:00 a.m. to 4:30 p.m. In total, the

employee spends 13 hours (6:00 a.m. to 12:30 p.m. and 4:30 p.m. to 11:00 p.m.) traveling to and from the worksite. However, the time between 8:00 a.m. and 12:30 p.m. is compensable as part of the employee's regular working hours. Also, an employee's time spent traveling outside of regular working hours to or from a transportation terminal (e.g., an airport or train station) within the limits of his or her official duty station is considered to be equivalent to commuting time and is not creditable travel time. (See 5 CFR 550.1404(d).) In this case, the employee spends 2 hours traveling to and from an airport within the limits of his official duty station.

In this example, the employee's compensatory time off for travel entitlement is as follows:

Total travel time	13 hours
<i>minus</i>	
Travel time within regular working hours	4.5 hours
Travel to/from airport within limits of official duty station	2 hours
Compensatory time off for travel	6.5 hours

Example 2: Travel to a temporary duty station on a nonworkday

Travel from home to a hotel on a Sunday

5:00 - 6:00 p.m.	6:00 - 7:30 p.m.	7:30 - 10:00 p.m.	10:00 - 10:30 p.m.
Drive to airport	Wait at airport	Plane departs/lands	Drive to hotel
<i>Noncreditable travel time</i>	<i>Creditable travel time</i>	<i>Creditable travel time</i>	<i>Creditable travel time</i>

Travel from a hotel to home on the following Saturday

6:30 - 7:00 a.m.	7:00 - 10:30 a.m.	10:30 a.m. - 1:00 p.m.	1:00 - 2:00 p.m.
Drive to airport	Wait at airport-2 hour delay	Plane departs/lands	Drive home
<i>Creditable travel time</i>	<i>Partially creditable travel time*</i>	<i>Creditable travel time</i>	<i>Noncreditable travel time</i>

An employee is required to travel to a temporary duty station for a week-long conference. The employee's regular working hours are 8:00 a.m. to 4:30 p.m., Monday through Friday. Because the conference begins early Monday morning, the employee travels to a hotel at the temporary duty station the Sunday evening before the conference. The conference is scheduled to continue into the evening on Friday, so the employee returns home on Saturday morning.

In total, the employee spends 13 hours (5:00 p.m. to 10:30 p.m. on Sunday and 6:30 a.m. to 2:00 p.m. on the following Saturday) traveling to and from the conference. However, the hour the employee spends on Sunday traveling to the airport and the hour the employee spends on Saturday traveling from

the airport within the limits of her official duty station is considered equivalent to commuting time and is not creditable time in a travel status.

*The agency's compensatory time off for travel policy allows up to 90 minutes of creditable waiting time at a transportation terminal. Therefore, only the time from 7:00 to 8:30 a.m. is creditable as "usual waiting time." (See 5 CFR 550.1404(b)(1).) The time from 8:30 to 10:30 a.m. is considered "extended waiting time" and is not creditable. (See 5 CFR 550.1404(b)(2).)

In this example, the employee's compensatory time off for travel entitlement is as follows:

Total travel time	13 hours
<i>minus</i>	
Travel to/from airport within limits of official duty station	2 hours
Extended waiting time	2 hours
Compensatory time off for travel	9 hours

Example 3: Travel from a temporary duty station on a workday (with cancelled connecting flight)

From temporary duty station to intervening airport for connecting flight on a Friday

5:30 - 6:30 a.m.	6:30 - 8:00 a.m.	8:00 - 11:00 a.m.	11:00 - 4:30 p.m.
Drive to airport	Wait at airport	Plane departs/lands	Connecting flight delayed due to severe weather. Flights are cancelled.
<i>Creditable travel time</i>	<i>Creditable travel time</i>	<i>Regular working hours</i>	<i>Regular working hours</i>

Employee checks into hotel near airport. No creditable travel time. Employee returns to airport on Saturday morning.

6:30 - 7:00 a.m.	7:00 - 8:30 a.m.	8:30 a.m. - 12:00 noon	12:00 noon - 1:00 p.m.
Drive to airport	Wait at airport	Plane departs/lands	Drive home
<i>Creditable travel time</i>	<i>Creditable travel time</i>	<i>Creditable travel time</i>	<i>Noncreditable travel time</i>

On a Friday (workday), an employee is required to travel from a temporary duty station to home. However, due to severe weather, the employee's connecting flight is cancelled until Saturday morning (nonworkday). On Friday, the employee's regular working hours are 8:00 a.m. to 4:30 p.m. In total, the employee spends 17.5 hours (5:30 a.m. to 4:30 p.m. on Friday and 6:30 a.m. to 1:00 p.m. on Saturday)

traveling from the temporary duty station. However, the time between 8:00 a.m. and 4:30 p.m. is compensable as part of the employee's regular working hours. (For the purpose of this example, we are assuming the employee has a 30-minute meal period during his regular working hours.) The extended waiting period from 4:30 p.m. until the employee departs for the airport on Saturday morning is not creditable travel time, since the employee is free to use the time for his own purposes. (See 5 CFR 550.1404(b)(2).) Also, an employee's time spent traveling outside of regular working hours to or from a transportation terminal (e.g., an airport or train station) within the limits of his or her official duty station is considered to be equivalent to commuting time and is not creditable travel time. (See 5 CFR 550.1404(d).) In this case, the employee spent 1 hour traveling from an airport within the limits of his official duty station.

In this example, the employee's compensatory time off for travel entitlement is as follows:

Total travel time	17.5 hours
<i>minus</i>	
Travel time within regular working hours	8.5 hours
Travel from airport within limits of official duty station	1 hour
Compensatory time off for travel	8 hours

Example 4: Driving to and from a temporary duty station on a workday

Travel to and from a training session

6:00 - 7:00 a.m.	7:00 - 8:00 a.m.	8:00 a.m. - 4:30 p.m.	4:30 - 5:30 p.m.	5:30 - 6:30 p.m.
Drive to training session	Drive to training session	Training	Drive home	Drive home
<i>Noncreditable travel time</i>	<i>Creditable travel time</i>	<i>Regular working hours</i>	<i>Noncreditable travel time</i>	<i>Creditable travel time</i>

An employee is required to travel to a temporary duty station on a workday for a 1-day training session. The training location is a 2-hour drive from the employee's home. The employee's regular working hours are 8:00 a.m. to 4:30 p.m. In total, the employee spends 4 hours (6:00 a.m. to 8:00 a.m. and 4:30 p.m. to 6:30 p.m.) driving to and from the training session.

If an employee travels directly between home and a temporary duty station outside the limits of his or her official duty station, the time spent traveling outside regular working hours is creditable travel time. However, the agency must deduct the time the employee would have spent in normal home-to-work/work-to-home commuting. (See 5 CFR 550.1404(c).) In this case, the employee's normal daily commuting time is 2 hours (1 hour each way). Therefore, 2 hours must be deducted from the employee's creditable travel time.

In this example, the employee's compensatory time off for travel entitlement is as follows:

Total travel time	4 hours
minus	
Normal commuting time	2 hours
Compensatory time off for travel	2 hours

Example 5: Travel to multiple temporary duty stations on a workday*Travel from home to first presentation site*

6:00 - 7:00 a.m.	7:00 - 8:00 a.m.	8:00 - 8:30 a.m.	8:30 - 10:00 a.m.	10:00 - 10:30 a.m.	10:30 - 12:00 noon
Drive to airport	Wait at airport	Wait at airport	Plane departs/lands	Drive to site	Presentation
<i>Noncreditable travel time</i>	<i>Creditable travel time</i>	<i>Regular working hours</i>	<i>Regular working hours</i>	<i>Regular working hours</i>	<i>Regular working hours</i>

Travel from first presentation site to second presentation site

12:00 noon to 12:30 p.m.	12:30 - 1:30 p.m.	1:30 - 2:30 p.m.	2:30 - 3:00 p.m.	3:00 - 4:30 p.m.
Drive to airport	Wait at airport	Plane departs/ lands	Drive to site	Presentation
<i>Regular working hours</i>	<i>Regular working hours</i>	<i>Regular working hours</i>	<i>Regular working hours</i>	<i>Regular working hours</i>

Travel from second presentation site to home

4:30 - 5:00 p.m.	5:00 - 6:30 p.m.	6:30 - 9:30 p.m.	9:30 - 10:30 p.m.
Drive to airport	Wait at airport	Plane departs/lands	Drive home
<i>Creditable travel time</i>	<i>Creditable travel time</i>	<i>Creditable travel time</i>	<i>Noncreditable travel time</i>

An employee is required to travel on a workday to two temporary duty stations to make presentations to stakeholders. The employee's regular working hours are 8:00 a.m. to 4:30 p.m. In total, the employee spends 13.5 hours traveling (6:00 a.m. to 10:30 a.m., 12:00 noon to 3:00 p.m., and 4:30 p.m. to 10:30 p.m.) between home and the two presentation sites. However, the time between 8:00 a.m. and 4:30 p.m. is compensable as the employee's regular working hours. (For the purpose of this example, we are assuming the employee has a 30-minute meal period during her regular working hours.) Also, the 2 hours the employee spends traveling outside of regular working hours to and from the airport within the limits of her official duty station is not creditable travel time.

In this example, the employee's compensatory time off for travel entitlement is as follows:

Total travel time	13.5 hours
<i>minus</i>	
Travel time within regular working hours	5.5 hours
Travel to/from airport within limits of official duty station	2 hours
Compensatory time off for travel	6 hours

 [Back to top](#)

[Return to Compensation Memoranda Main Page](#)

This page can be found on the web at the following url: <http://archive.opm.gov/oca/compmemo/2005/2005-03-att2.asp>

U.S. Office of Personnel Management

1900 E Street, NW, Washington, DC 20415 | (202) 606-1800 | TTY (202) 606-2532



**DEFENSE CRIMINAL INVESTIGATIVE SERVICE
COMPENSATORY TIME OFF FOR TRAVEL APPROVAL FORM**



NAME (Last, First)		fdfldj		Normal Duty Hours				Normal Commute Time ¹ (in Hours - i.e. 1.0, .75, .50 or .25)						
Destination				Departure Date				Return Date						
Outbound Travel		Time Zone	Departed	Time Credited in 15 minute increments										
	Travel Segment	Depart Time	Arrival Time	Total Hrs.	-	Paid Hours ⁵	-	Unusual Wait Time	-	Commute Time	-	Meals ⁴	=	Travel Comp Hours
Line 1	Home / Worksite to Transportation Terminal or TDY Worksite / Hotel ¹			0.00	-		-		-		-		=	0.00
Line 2	Waiting Time Between Legs ²			0.00	-		+		-		-		=	0.00
Line 3	Time in Travel ³			0.00	-		-		-		-		=	0.00
Line 4	Waiting Time Between Legs ²			0.00	-		+		-		-		=	0.00
Line 5	Time in Travel ³			0.00	-		-		-		-		=	0.00
Line 6	Waiting Time Between Legs ²			0.00	-		+		-		-		=	0.00
Line 7	Time in Travel ³			0.00	-		-		-		-		=	0.00
Line 8	Waiting Time ²			0.00	-		+		-		-		=	0.00
Line 9	Transportation Terminal to TDY Work Site / Hotel ¹			0.00	-		-		-		-		=	0.00
				Total Travel Hours	0.00								=	0.00
Return Travel (Inbound)		Time Zone	Departed	Time Credited in 15 minute increments										
	Travel Segment	Depart Time	Arrival Time	Total Hrs.	-	Paid Hours ⁵	-	Unusual Wait Time	-	Commute Time	-	Meals ⁴	=	Travel Comp Hours
Line 1	Home / Worksite to Transportation Terminal or TDY Worksite / Hotel ¹			0.00	-		-		-		-		=	0.00
Line 2	Waiting Time Between Legs ²			0.00	-		+		-		-		=	0.00
Line 3	Time in Travel ³			0.00	-		-		-		-		=	0.00
Line 4	Waiting Time Between Legs ²			0.00	-		+		-		-		=	0.00
Line 5	Time in Travel ³			0.00	-		-		-		-		=	0.00
Line 6	Waiting Time Between Legs ²			0.00	-		+		-		-		=	0.00
Line 7	Time in Travel ³			0.00	-		-		-		-		=	0.00
Line 8	Waiting Time ²			0.00	-		+		-		-		=	0.00
Line 9	Transportation Terminal to TDY Work Site / Hotel ¹			0.00	-		-		-		-		=	0.00
				Total Travel Hours	0.00								=	0.00
Traveler's Signature		Date		Total Travel Comp Time Earned										0.00
Approving Official's Signature		Date		1. Attach Travel Itinerary (Optional if available) 2. Submit to approving Official 3. Forward to Timekeeper for retention, or attached in DAJ										

1) Deduct commute time, if applicable:
DCI FORM 0072010

Commuting Time is defined as:

(a) Commuting outside an employee's regular work hours between an employee's home and a temporary duty station or transportation terminal outside the limits of the official duty station is considered creditable travel time. Though the employee's normal home-to-work/work-to-home commuting time will be deducted from the creditable travel time.

ENTER YOUR NORMAL COMMUTE TIME in 15 minute increments (e.g., .25, .5, .75, 1.0).

(b) Commuting outside of regular working hours between home and a transportation terminal within the limits of the employee's official duty station is considered equivalent to commuting time and is not creditable travel time.

ENTER YOUR NORMAL COMMUTE TIME in 15 minute increments (e.g., .25, .5, .75, 1.0).

(c) Travel outside of regular working hours between a worksite and a transportation terminal is creditable travel time, and no commuting time offset applies. **((DO NOT ENTER COMMUTE TIME))**

Only travel for formal training/conference attendance scheduled in advance is eligible for Comp Time for Travel. Travel in connection with investigative activity is NOT creditable as Comp Time for Travel, and hours in excess of regular hours must be charged as LEAP.

2) Anything exceeding 2 hours must be recorded as Unusual Wait Time.

The maximum, creditable time allowed for usual waiting time at a transportation terminal for one leg on a domestic flight is two (2) hour, or 3 hours for international flights. (See Definitions)

3) Compensatory time for travel cannot be credited during an employee's regular working hours.

4) Meals: Do not deduct for a 30 minute unpaid meal time if travelling on a Regular Day Off. Agents need not specify Meal times.

5) Paid Hours: Regular hours worked and any hours that fit under hours of work conditions regular duty hours. 10 hours (8 hours regular time and 2 hours LEAP) is to be listed for travel that occurs during the Agent's regularly scheduled workday (Tour of Duty).

All other employees, and Agents not claiming LEAP due to 4 or more hours of training (exempt day) would list 8 hours of regular duty hour's time.

DEFINITIONS

Usual waiting time: This pertains to travel outside of regular work hours only. It is time spent waiting at the transportation terminal to include early arrival for check-in purposes. If the connecting transportation is delayed or cancelled, i.e., the flight is cancelled and the employee arrives at a local hotel, the time between arriving at the local hotel until his/her departure from the local hotel to return to the transportation terminal to resume travel is not considered usual waiting time and is not creditable for compensatory time off.

Determinations regarding what is creditable as "usual waiting time" are within the sole, and exclusive discretion of the SAC/ASAC/RAC.

Travel Status: Defined as the time an employee actually spends traveling between the official duty station and a temporary duty station, or between two temporary duty stations, and the unusual waiting time that precedes or interrupts such travel.

Time spent at a temporary duty station between arrival and departure is not time in a travel status.

Meals: Do not deduct for a 30 minute unpaid meal time if travelling on a Regular Day Off. Agents need not specify Meal times.

CHAPTER 55

INSPECTIONS

<u>Contents</u>	<u>Section</u>
General	55.1
Definitions	55.2
Objectives	55.3
Self-Inspections	55.4
Verification Inspection Procedures	55.5
Scheduling	55.6
Inspection Team Composition	55.7
Duties of Inspectors	55.8
Inspection Timeline	55.9
Verification Reporting and Follow-up	55.10
Manager's Internal Control Procedures	55.11
Attachments for Verification Inspections	55.12

55.1. General

55.1.a. This chapter provides policies and general procedures for the Department of Defense Office of Inspector General (DoD OIG), Defense Criminal Investigative Service (DCIS) inspections program.

55.1.b. The DoD Instruction 5010.40, "Managers' Internal Control Program Procedures," May 30, 2013, provides DoD internal policy, responsibilities, procedures, and reporting requirements for establishing and maintaining DoD Component Managers' Internal Control (MIC) Programs. The OIG MIC Program extends to every responsibility and activity undertaken by the OIG and is applicable to financial, administrative, program, and operational controls. The nature of the mission of the OIG requires an internal commitment to measure performance and examine the adequacy of MICs to ensure that high quality performance is completed efficiently and effectively. The DCIS Inspections Program assists in maintaining the OIG MIC Program.

55.1.c. In June 2010, the Council of the Inspectors General on Integrity and Efficiency (CIGIE) officially adopted the "Quality Standards for Inspections" as the professional standards for all inspection and evaluation work performed by member organizations. The Inspector General Reform Act of 2008 requires compliance with these standards. The Government Accountability Office currently uses the CIGIE standards to evaluate statutory OIG investigative and audit operations. The DoD Inspector General (IG) has directed that DCIS will comply with applicable standards developed by the CIGIE Quality Standards for Investigations.

55.1.d. The DCIS Headquarters (HQ) Internal Operations Directorate (Internal Operations) manages the DCIS inspections program. It has the responsibility for scheduling,

organizing, and conducting inspections and testing internal controls of DCIS components and programs; ensuring inspection reports are prepared and reviewed for compliance with CIGIE and other guidelines as specified by the DoD OIG, the Deputy Inspector General for Investigations (DIG-INV), or both; ensuring that reports are centrally recorded; and ensuring inspection findings are satisfactorily corrected.

55.1.e. Management personnel are required to conduct self-inspections of their offices prior to a DCIS verification inspection (VI) as outlined in the appropriate attachments to this chapter. DCIS VIs are not a substitute for an OIG Office of Quality Assurance and Standards (QAS) quality assurance review of a specific management program.

55.2. Definitions

55.2.a. **Statement of Assurance (SOA).** An annual statement in memorandum format provided to the DoD IG that reflects a leader's explicit level of assurance on whether internal controls are effective. The SOA is based on the results of self-inspections, verification inspections, program inspections conducted for mission-essential functions relative to risk, and external quality assurance reviews and inspections. It also identifies material weaknesses found during inspections.

55.2.b. **Verification Inspection.** A regularly scheduled inspection of a DCIS Field Office or DCIS HQ facilitated by Internal Operations.

55.2.c. **Self-Inspection.** An inspection of a DCIS Field Office or DCIS HQ conducted under the direction of a senior manager of the inspected office, prior to a verification inspection by Internal Operations.

55.2.d. **Program Inspection.** An inspection of a DCIS program conducted by an external stakeholder outside of DCIS such as QAS or a CIGIE Qualitative Assessment Review (Peer Review). (Refer to QAS Chapter 3 for program inspection procedures).

55.2.e. **Field Office and All Subordinate Offices.** All DCIS Field Offices, Resident Agencies, Posts of Duty, and any other office not physically collocated at DoD OIG HQ.

55.2.f. **Action Item.** A deficiency that requires a written response on actions taken to correct the deficiency.

55.2.g. **Repeat Action Item.** An action item reported in a previous inspection that exists again during a current inspection. Management must explain the reason for any repeat action items.

55.3. Objectives. The objectives of the DCIS Inspections Program are to evaluate whether HQ and field elements are:

55.3.a. operating in compliance with relevant laws, regulations, standards, policies, and established procedures;

55.3.b. managing and using resources in an efficient and economical manner;

55.3.c. properly accounting for all cash expenditures and funds;

55.3.d. identifying ways to streamline or improve agency processes; and

55.3.e. managing, administering, and conducting DCIS programs in accordance with established guidelines, policies, and directives.

55.4. Self-Inspections

55.4.a. **Purpose.** The self-inspection program is intended to provide the maximum opportunity for timely and consistently applied reviews by management in each DCIS office. Through regular self-inspection, the primary managers in these offices will be able to monitor and improve operations and administration and correct deficiencies. Improved operational methods or procedures that would benefit other offices shall be identified and presented by Internal Operations to appropriate management officials for organizational implementation. The self-inspection program is intended to help provide a more uniform, timely, and consistent internal management control program for DCIS.

55.4.b. **Responsibilities.** DCIS senior managers are responsible for ensuring DCIS field offices, subordinate elements, and all directorates are inspected in accordance with the requirements of this chapter (See Attachments A through D). Senior managers have the authority to determine who will complete the self-inspection for their respective offices and when it will be done. However, in order to maintain the integrity of the inspection program, whenever possible, each office should be inspected by personnel not assigned to the office being inspected.

55.4.c. **Self-Inspection Procedures.** All self-inspections will be conducted using the following guidelines.

55.4.c.(1). **Inspection Checklists.** Use the following inspection checklists for conducting self-inspections of DCIS offices.

55.4.c.(1).(a). Checklists 1 through 18 of Attachment D for self-inspections of DCIS field offices and all subordinate offices, including self-inspections of DCIS HQ. (Note: Checklist page numbers ending with an “A” are for inspections of field locations, and checklist page numbers ending with a “B” are for inspections of DCIS HQ. Checklists with no letter after the page number are for inspections of either the field only, DCIS HQ only, or both the field and HQ. See page 55-D-1.)

55.4.c.(2). **Inspection Summary.** The individual assigned responsibility for the self-inspection will prepare a summary of each office inspected. The self-inspection will cover the core areas identified in the inspection checklists. The summaries, action items, and any other pertinent information developed during the inspection will form the basis for the self-inspection report.

55.4.c.(3). **Self-Inspection Report.** The self-inspection report and all required attachments must be received by the Program Manager (PM) for Inspections and Compliance no later than 60 calendar days prior to the beginning of the verification inspection. Forward the

self-inspection report as an email attachment in MS Word format. The signed transmittal page should be scanned as an Adobe Acrobat .pdf file and forwarded as a second attachment to the email. All original inspection checklists and notes prepared during the self-inspection must be forwarded at the time the self-inspection report is submitted. Copies of the completed inspection checklists and notes may be retained in the inspected office until the verification inspection is completed and until the completion of the next CIGIE Peer Review. The self-inspection report will be prepared using formats provided in the appropriate attachments (Attachments A through D), and will include the elements listed below.

55.4.c.(3).(a). Transmittal Memorandum. Identify the office to which the report pertains, the dates of inspection, the preparers, and the approving official.

55.4.c.(3).(b). Executive Summary. This one to four page section should provide a concise picture of the field office or HQ directorate being described and, in particular, should focus on effectiveness and efficiency. List the individuals who conducted the self-inspection at each office. The following areas should be considered when preparing this portion of the report: (1) executive management, (2) investigative prioritization, and (3) administrative support.

55.4.c.(3).(c). Action Items. Identify deficiencies that require corrective actions, the corrective actions taken or proposed, the responsible person or persons, and the anticipated dates of completion. Action items will be grouped by the office to which they pertain. Action items may range from minor items requiring very simple corrective actions to more serious issues, such as identification of areas that are not functioning in accordance with established policies and are adversely affecting the efficiency or effectiveness of the inspected office, or flagrant disregard for established rules. Follow the format for Action Items in the appropriate attachment (Attachment A through D). List each office separately, and begin each office on a new page.

55.4.c.(3).(c).1. If the issue requires coordination with or action by a support Component within the DoD OIG, the PM for Inspections and Compliance will forward the information to the responsible Component head to ensure the issue is addressed. If the inspected office has had previous correspondence with an office regarding the issue, attach copies of the correspondence to the action items.

55.4.c.(3).(c).2. Identify any necessary corrective action to be taken for each action item. Include the identity of the manager of the office where the corrective action is required, the supervisor responsible for implementation or coordination of the corrective action, and the anticipated date of completion.

55.4.c.(3).(d). Manager Profiles. Each manager is required to complete a three-question manager profile listing their noteworthy accomplishments since the last inspection, rating their effectiveness as a manager, and describing their career goals.

55.4.c.(3).(e). Collateral Duty Assignments. Complete Attachment B for each office or include a copy of an existing collateral duty assignment memorandum. Place all collateral duty assignment memorandums together following the Action Items section of the report.

55.4.c.(3).(f). Miscellaneous Items. Discuss any items that the senior manager wishes to bring to the attention of the PM for Inspections and Compliance.

55.5. Verification Inspection Procedures

55.5.a. Entrance Briefing

55.5.a.(1). **Verification Inspections**. The Special Agent in Charge (SAC), Assistant Inspector General (AIG), field manager, or designee will brief the inspection team concerning information not provided in the self-inspection report. Information required may be found in Attachment D.

55.5.b. The Inspection

55.5.b.(1). **Verification Inspections**. Generally, the elements to be inspected will be identical to elements inspected during the self-inspection and the inspection team will focus its efforts on the following:

55.5.b.(1).(a). areas identified in the self-inspection report as needing attention or correction;

55.5.b.(1).(b). elements of the inspection checklist indexes chosen at random;

55.5.b.(1).(c). areas as directed by senior management;

55.5.b.(1).(d). areas identified by the SAC, AIG, or field manager of the office being inspected; or

55.5.b.(1).(e) areas identified by Internal Operations or senior management as needing attention or correction.

55.5.c. **Inspection Elements**. The elements of all inspections shall consist of those laws, directives, or regulations that are applicable to the inspected office or program. Generally, those portions of the DCIS Special Agents Manual, DoD and DoD IG directives and instructions, CIGIE Quality Standards for Investigations, or similar guidance for program inspections, as appropriate, shall be used in each inspection.

55.5.d. Use of Inspection Checklists

55.5.d.(1). **Inspections**. The inspection checklists have been developed as tools for management and inspectors. The checklists and any notes completed by inspectors, as well as any supporting documentation, will constitute the backup documentation to the inspection

report. The PM for Inspections and Compliance will coordinate any changes to inspection checklists on an ongoing basis to reflect changes in applicable guidance, agency policy, or management priorities. Revised checklists will be issued with the approval of the AIG for Investigations (AIGI), Internal Operations. Additional items may be included with the inspection announcement.

55.5.e. Post-Inspection Analysis. Inspection observations and results will be discussed with the SAC or Assistant Special Agent in Charge (ASAC) of the inspected office or program at the conclusion of the inspection. The discussion provides an opportunity for supervisory personnel to comment or clarify circumstances concerning the inspection findings before the inspection report is prepared. Results of each inspection will be briefed to the DIG-INV or AIGI as soon as practicable following the inspection.

55.5.f. Techniques

55.5.f.(1). In support of the objectives cited above, the members of the inspection team shall concentrate on those areas that are manifestly important or that require action.

55.5.f.(2). The inspectors' inquiries shall include, but not be limited to, the following:

55.5.f.(2).(a). planning, performance, and productivity in relation to the mission of the inspected office or program;

55.5.f.(2).(b). whether the inspected office or program management staffing should be augmented, reduced, or consolidated to ensure the most effective use of personnel or execution of the program;

55.5.f.(2).(c). pertinent aspects of leadership, management, use of resources, and training; and

55.5.f.(2).(d). application of investigative or other organizational priorities.

55.5.f.(3). The inspection inquiries shall include discussions with knowledgeable personnel concerning topics such as:

55.5.f.(3).(a). plans or projects that have or will result in increased effectiveness or reduced costs;

55.5.f.(3).(b). situations or practices that actually or potentially detract from mission performance;

55.5.f.(3).(c). current problems that require assistance from a higher management level, support offices within the OIG, or external organizations; and

55.5.f.(3).(d). functions or tasks levied on the inspected office without sufficient resources.

55.6. Scheduling

55.6.a. DCIS HQ and each DCIS Field Office will be inspected once every 3 years. The frequency of inspections may be revised to meet staffing limitations and other mission requirements. Approximately 4 to 6 months prior to a verification inspection, the PM for Inspections and Compliance will establish specific inspection dates with the SAC or AIG of the office to be inspected.

55.6.b. The DIG-INV or AIGI, Internal Operations, may direct an inspection of any office or program at any time. The PM for Inspections and Compliance may also identify a program for an inspection resulting from information developed during misconduct investigations or other sources. When this occurs, Internal Operations may modify inspection procedures, the inspection schedule, or both to accommodate the inspection.

55.7. Inspection Team Composition

55.7.a. The PM for Inspections and Compliance will coordinate, facilitate, and oversee the inspection teams.

55.7.b. The PM for Inspections and Compliance is responsible for coordinating and leading the inspection, interfacing with the SAC or AIGI of the inspected office or program, interfacing with respective VI Team Leaders, collecting team member write-ups, providing briefings to team members, and preparing the inspection reports.

55.7.c. Inspection teams will consist of DCIS personnel selected from various HQ and field elements, when necessary. Depending on the key areas being inspected, personnel from other DoD OIG components could be part of the VI team. The size of the office or program to be inspected, the complexity of the workload, and locations of subordinate offices will be used in determining the number and qualifications of personnel assigned to the inspection team. Because VIs could be geographically dispersed, the PM will designate a Team Leader for the VI locations. The VI Team Leader will be the conduit between the PM and the senior official of the location being inspected. The VI Team Leader will be responsible for collecting and providing team member write-ups, checklists, and inspection reports to the PM. The AIGI Internal Operations is the final authority on the composition of each inspection team.

55.8. Duties of Inspectors

55.8.a. DCIS inspection team members do not have supervisory authority over the offices or programs being inspected. During the course of the inspection, inspectors shall guard against actions that could be interpreted as an attempt to exercise such authority. The inspectors may suggest corrective actions and techniques or procedures for improved efficiency. However, only the inspection report shall be directive in nature and require corrective action and a written response from management.

55.8.b. Inspectors should perform the following basic evaluation duties.

55.8.b.(1). Identify exemplary performance or innovative procedures and techniques that will benefit or improve the organization.

55.8.b.(2). Identify problems, non-adherence to policy or established procedures, and report all relevant facts.

55.8.b.(3). Provide necessary background information to assist reviewers in an analysis of the facts.

55.8.b.(4). Recommend corrective action, improvements, or both.

55.8.b.(5). Maintain all inspection-related information in strictest confidence.

55.8.c. In order to carry out these duties effectively, inspectors, at a minimum, shall prepare themselves in advance by:

55.8.c.(1). taking part in all briefings prior to the inspection;

55.8.c.(2). studying the geographic jurisdiction, resources, and assigned tasks of the offices to be inspected;

55.8.c.(3). becoming familiar with existing guidance, policies, and procedures of any programs to be inspected;

55.8.c.(4). conducting a thorough analysis of the workload of the offices to be inspected; and

55.8.c.(5). reviewing previous inspection reports concerning the office or program to be inspected.

55.9. Inspection Timeline

55.9.a. Verification Inspections

55.9.a.(1). Approximately 13 weeks prior to a scheduled verification inspection, the PM for Inspections and Compliance will solicit inspection team volunteers. Inspection team members will be notified of their selection approximately 9 weeks prior to the inspection.

55.10. Verification Reporting and Follow-up

55.10.a. Verification Inspection Report

55.10.a.(1). **Verification Inspections.** Internal Operations will publish a draft inspection report within 8 weeks from the completion of the inspection. The inspection report will normally contain the following headings:

55.10.a.(1).(a). Entrance Briefing

55.10.a.(1).(b). Inspection Observations

55.10.a.(1).(c). Manager Interviews

55.10.a.(1).(d). Employee Interviews

55.10.a.(1).(e). Inspection Results

55.10.a.(1).(f). Employee Suggestions

55.10.a.(1).(g). Exhibits

55.10.a.(1).(h). SAC, ASAC, or AIGI Comments

55.10.a.(2). All items that are not in compliance or are of significant interest shall be addressed separately in a clear, succinct discussion of the issues. Recommendations shall be reasonable, pertinent to a specific problem or improvement, and clearly articulated. When a draft report is published, recommendations shall propose the office or offices responsible for correcting the issue.

55.10.a.(3). A cover memorandum from the PM for Inspections and Compliance shall be used to transmit draft inspection reports to the DIG or appropriate AIG through the Program Director (PD) and Deputy AIGI (DAIGI). Additionally, an excerpt from the draft inspection report listing only those action items that require input or assistance from supporting offices within the DoD OIG will be transmitted to the DIG or AIG of the supporting office using similar cover memorandums.

55.10.a.(4). All transmittal memorandums and written reports shall be marked "For Official Use Only." Reports and memorandums containing classified information shall be identified in accordance with Executive Order 12356, "National Security Information," April 2, 1982, and DoDM 5200.01, Volume 2, "DoD Information Security Program: Marking of Classified Information," Change 2, March 19, 2013. The first page of both draft and final inspection reports shall include the following caveat identifying the privileged nature of the material:

This inspection report was prepared by the Inspections and Compliance Unit, Internal Support Directorate, Internal Operations Directorate and is intended strictly for the use of the addressee. Further dissemination of this report requires the specific authorization of the AIGI-Internal Operations.

55.10.b. Follow-up

55.10.b.(1). The SAC or AIGI of the inspected office or having oversight responsibilities for the inspected program will provide the PM for Inspections and Compliance through the PD for Internal Support and DAIGI for Internal Operations with a written response to the draft report. Comments should state the actions taken, in progress, or proposed to correct all deficiencies and satisfy all recommendations listed in the draft report. For verification inspections, comments are due within 8 weeks of the receipt of the draft inspection report, or in the case of support offices, comments are due within 8 weeks of the receipt of an excerpt from the draft report.

55.10.b.(2). The SAC or AIGI of the inspected office and any support offices is not restricted to the recommendations and suggestions listed in the draft report. They may use them as a partial or complete solution, or may develop an alternative solution to the issue. Regardless of the procedure, the issues and concerns identified in the inspection report must be corrected in accordance with all applicable policies and procedures and approved by the AIGI-Internal Operations and the DIG-INV.

55.11. Managers' Internal Control Procedures

55.11.a. Risk Assessment

55.11.a.(1). In accordance with DoDI 5010.40, the DCIS will test internal controls, conduct inspections and verifications, and render assessments on what the DIG-INV has identified as risk areas, while regional offices routinely self-inspect those risk areas. The risk of error or inability to accomplish mission objectives was derived from a level of materiality based upon management's judgment to include the following criteria: 1) potential for loss of life or detriment to health and safety; 2) potential waste and abuse of taxpayers' money; 3) potential for a national security breach; 4) potential for impact, exposure, or impediment to a criminal investigation; and 5) potential for adverse impact of the agency's credibility or integrity. The DCIS Inspections Program assists in maintaining the DoD OIG MIC Program.

55.11.b. Assessable Unit Manager

55.11.b.(1). DCIS will appoint the PM for Inspections and Compliance as the agency's assessable unit manager (AUM), as a collateral duty in writing, within 90 days of becoming PM. The AUM will be responsible for establishing and implementing the DCIS MIC Program in accordance with the procedures detailed in DoD Instruction 5010.40.

55.11.b.(2). The DCIS AUM will complete the annual SOA in memorandum format provided to the Inspector General that reflects the DIG-INV's explicit level of assurance on whether internal controls are effective. The SOA is based on self-inspections, verification inspections, and program inspections conducted for mission-essential functions relative to risk. It also identifies material weaknesses found during the inspections.

55.11.b.(3). The DCIS AUM will:

55.11.b.(3).(a). identify and test internal controls;

55.11.b. (3).(b). recommend improvements based on best practices and feedback;

55.11.b.(3).(c). enhance controls and eliminate inefficient controls;

55.11.b.(3).(d). ensure agency Subject Matter Experts (SMEs) assess risk that may adversely affect the DCIS mission or operation;

55.11.b.(3).(e). assist in testing, as needed, and validating conclusions provided by SMEs;

55.11.b.(3).(f). identify and classify program deficiencies based on evaluations conducted;

55.11.b.(3).(g). assist SMEs in ensuring corrective action plans are developed to address program deficiencies;

55.11.b.(3).(h). ensure identified efficiencies, best practices, or deficiencies are shared across the agency;

55.11.b.(3).(i). track the progress of corrective action plans;

55.11.b.(3).(j). coordinate with the PM for Investigative Policy and the SMEs to provide recommendations for the enhancement, elimination, or implementation of a policy as a result of an inspection finding; and

55.11.b.(3).(k). report deficiencies for consideration of their impact on the organization and consideration of inclusion as a weakness in the organization's SOA.

55.11.c. **MIC Process**

55.11.c.(1). The MIC process will be integrated into the daily management practices of all managers and will:

55.11.c.(1).(a). Address all significant operations and mission responsibilities and not limit evaluations to operations applicable to financial management.

55.11.c.(1).(b). Be designed, documented, and operated to provide reasonable assurance that the specific standards and objectives enumerated in references (c) and (d) of DoDI 5010.40 are met.

55.11.c.(1).(c). Require managers to continuously monitor and improve the effectiveness of vital MICs.

55.11.c.(1).(d). Provide the basis for the annual SOA.

55.11.c.(2). **Methodologies.** The DCIS AUM or agency managers may also use sampling and testing methodologies for ensuring internal controls of inspection processes and results. Samples can be selected randomly or non-statistically. Testing methods can include a general inquiry, orally or in writing, of the personnel involved in the execution of a program; observation, examination, or inspection of actual controls in operation; reviewing evidence of a given procedure; or the request for reperformance of a control activity to obtain sufficient evidence of its operating effectiveness. Two or more testing methodologies can also be combined.

55.11.c.(3). **Assessable Units.** All programs and operations of DCIS will be segmented along organizational, functional, or programmatic lines into assessable units (inspection checklist items). DCIS HQ will establish and maintain an inventory of its assessable units. The inventory will be a part of the DCIS MIC Plan and will be reviewed and updated as

necessary, along with the control objectives, control techniques, and control tests within each assessable unit.

55.11.c.(4). **Evaluation.** Evaluate the effectiveness of the MICs through a documented process or mechanism determined by DCIS to meet agency specific requirements. The evaluations will be consistent with the guidance contained in references (a) and (d) of DoDI 5010.40. The process should maximize the use of already existing management evaluation data and, to the greatest extent possible, minimize the creation of processes solely for the execution of the MIC Program.

55.11.c.(5). **Annual SOA Submission.** DCIS will submit an Annual SOA to the AIG-QAS, based on a general assessment of the effectiveness of its inspections program. The statement will include material weaknesses and the plan to correct them, and be consistent with annual QAS guidance about the content and structure of the statement. The statement must be signed by the DIG-INV and submitted to the AIG-QAS at least one month before the date the DoD OIG Annual SOA is due to the Secretary of Defense.

ATTACHMENTS

- A. Self-Inspection Report and Manager Profiles
- B. Collateral Duty Assignments
- C. Miscellaneous Items
- D. Checklist Index and Inspection Checklists (Note: Checklist page numbers ending with an “A” are for inspections of field locations, and checklist page numbers ending with a “B” are for inspections of DCIS HQ. Checklists with no letter after the page number are for inspections of either the field only, DCIS HQ only, or both the field and HQ. See page 55-D-1.)

ATTACHMENT A

SELF-INSPECTION REPORT AND MANAGER PROFILES



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
DEFENSE CRIMINAL INVESTIGATIVE SERVICE
FIELD OFFICE NAME
FIELD OFFICE ADDRESS
CITY, STATE ZIP

MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL FOR INVESTIGATIONS, INTERNAL OPERATIONS

Month, xx, 20xx

SUBJECT: Transmittal of Self-Inspection Report

During the period _____, members of the _____ Field Office/Directorate management staff conducted a self-inspection of the _____ Field Office/Directorate. I have personally reviewed the resultant report, and I certify that the _____ Field Office/Directorate inspection was completed in a thorough manner in accordance with established procedures. The report is attached for your review and such actions as may be appropriate.

Name
Special Agent in Charge

Attachment:
As stated

ATTACHMENT A

_____ FIELD OFFICE/DIRECTORATE SELF-INSPECTION
MONTH, DAY, YYYY, THROUGH MONTH, DAY, YYYY

Table of Contents

	Page
Executive Summary	
Background (optional)	
Action Items	
Manager Profiles	
Collateral Duty Assignments	
Original Inspection Checklists	

ATTACHMENT A

EXECUTIVE SUMMARY

During the period (Month Day, Year), through (Month Day, Year), the _____ Field Office/Directorate conducted its self-inspection. This self-inspection covered the period since the last inspection. It measured both the efficiency of the various programs and functions reviewed, and the overall effectiveness of the field office enforcement program. The following individuals conducted the self-inspection at the offices indicated:

(List inspectors and the offices they inspected)

Administrative and support activities are being carried out in an efficient and competent manner. In addition to the action item(s) listed above, there were an additional ## action items relating to [confidential source file management, investigative case file management, evidence, and emergency and extraordinary funds] identified during this inspection. ## of these issues will be addressed by the _____ Field Office/Directorate and ## requires action on the part of _____ (list the Headquarters element(s)).

ATTACHMENT A

BACKGROUND

The _____ Field Office/Directorate components include the _____, _____ and _____ (Resident Agencies (RAs) with Posts of Duty (PODs) in _____. The last inspection of this Field Office/Directorate was conducted during the period _____ through _____. At that time the _____ Field Office/Directorate was authorized _____ special agents and _____ administrative support personnel. The current authorization is a total of _____ DCIS employees (a significant increase/decrease from the last inspection).

Between _____ and _____, the _____ Field Office/Directorate conducted the enclosed self-inspection.

Authorized On-Board

Special Agents
Administrative Support

Total

Field Office/Directorate Management

_____ has been the Special Agent in Charge (SAC) of the _____ Field Office/Directorate since _____. Prior to assuming this position, SAC _____ held several managerial positions in the field and DCIS Headquarters, the last being _____.

Assistant Special Agent in Charge (ASAC) _____, who assumed this position in _____, also manages the Field Office. ASAC _____ was assigned to _____ prior to assuming (his/her) present position. The _____ Resident Agents in Charge (RACs) and Supervisory Special Agents (SSAs) report directly to ASAC _____. They are _____ since _____, _____ since _____ and _____ since _____.

(Provide information regarding any unique problems regarding operational or administrative issues confronting the Directorate/Field Office, Resident Agencies, or Posts of Duty. Further, synopsise significant efforts in developing and initiating investigations in conjunction with the organization's prioritized goals and objectives.

ATTACHMENT A

(Begin each office on a new page.)

Action Items ABC Field Office/ABC Resident Agency

4 – CRIMS Data Integrity Review

List the first finding here, followed by the Corrective Action and Completion Date (see below). Identify the CN of each finding so corrective action can be verified during the verification inspection. After listing the first finding, Corrective Action, and Completion Date, list the next finding in the same format. Each finding must list a Corrective Action and a Completion Date.

Corrective Action:

SAC Doe has tasked ASAC Smith to coordinate with _____ (whoever is responsible for fixing the action item) and ensure _____ (list the corrective action to be taken here).

Completion Date: (Enter the estimated completion date. It will usually be within 60 days of submission of the Field Office Self-Inspection report to the Director of Inspections. Normally all findings should be corrected before the verification inspection team arrives, but there may be circumstances where that won't be the case.)

5 – Evidence Review

List the first finding here, followed by the Corrective Action and Completion Date (see below). After listing the first finding, Corrective Action, and Completion Date, list the next finding in the same format. Each finding must list a Corrective Action and a Completion Date.

Corrective Action:

SAC Doe has tasked ASAC Smith to coordinate with _____ (whoever is responsible for fixing the action item) and ensure _____ (list the corrective action to be taken here).

Completion Date:

Continue for each checklist item where an action item exists. If there are no action items for a particular checklist item, do not list that checklist item.

List enough identifying data (e.g., CN, pay period ending date, evidence log entry number, serial number, vehicle license plate number) so that the corrective action can be verified by a verification inspection team member.

ATTACHMENT A

MANAGER PROFILE: First/Last Name

Position:

Office:

DCIS EOD:

Length of time in current position:

Describe noteworthy accomplishments:

How does the manager perceive his effectiveness in relating with supervised personnel and outside agencies:

Describe the manager's career goals and plans: (Include sentence about retirement eligibility/plans)

ATTACHMENT B

COLLATERAL DUTY ASSIGNMENTS

(Use the following or attach assignment memorandum.)

Office _____

<u>Duty</u>	<u>Primary</u>	<u>Alternate</u>
Firearms Coordinator	_____	_____
Control Tactics Coordinator	_____	_____
Health and Wellness Coordinator	_____	_____
Undercover Coordinator	_____	_____
Source Control Officer	_____	_____
Security Officer	_____	_____
Top Secret Control Officer	_____	_____
Classified Document Custodian	_____	_____
Motor Vehicle Control Officer	_____	_____
Training Officer	_____	_____
E&E Fund Custodian	_____	_____
Government Purchase Card Holder(s)	_____	_____
Property Custodian	_____	_____
Technical Equipment Officer	_____	_____
Evidence Custodian	_____	_____
Grand Jury Material Custodian	_____	_____
Admin. File Custodian	_____	_____
Timekeeper	_____	_____
TECS	_____	_____
Other	_____	_____
Other	_____	_____

ATTACHMENT C
MISCELLANEOUS ITEMS

(Add any additional items, if appropriate)

ATTACHMENT D

CHECKLIST INDEX AND INSPECTION CHECKLISTS

CHECKLIST INDEX

I. SAC/ASAC/RAC ENTRANCE BRIEFING (VI only)	(HQ and Field)
II. SPECIAL AGENT INTERVIEWS (VI only)	(II.A-Field, II. B-HQ)
III. NON-AGENT INTERVIEWS (VI only)	(Field and HQ)
IV. PROGRAM CHECKLISTS: Self and Verification Inspections (VI)	
1. Evidence Custody System	(Field)
2. Subpoenaed Material	(Field)
3. Emergency and Extraordinary (E&E) Funds	(3A-Field, 3B-HQ)
4. Undercover Operations	(4A-Field, 4B-HQ)
5. Confidential Informants	(5A-Field, 5B-HQ)
6. Classified Documents	(Field and HQ)
7. Interception of Wire, Electronic & Oral Communications	(7A-Field, 7B-HQ)
8. Technical Services Program/Radio Communications	(8A-Field, 8B-HQ)
9. Agent Gear, Badge, and Credentials Accountability	(Field and HQ)
10. Weapons and Ammunition	(Field and HQ)
11. Case File and CRIMS	(11A-Field, 11B-HQ)
12. Health and Wellness Program	(Field and HQ)
13. Training Programs	(Field and HQ)
14. Administrative Files	(14A-Field, 14B-HQ)
15. Government Owned Vehicles	(Field and HQ)
16. Asset Forfeiture Program	(HQ)
17. Coordination of Remedies	(HQ)
18. Cyber Field Office	(CYBER FO only)

CHAPTER 56

BLOODBORNE PATHOGENS AND TUBERCULOSIS

<u>Contents</u>	<u>Section</u>
Purpose	56.1.
General	56.2.
Scope and Applicability	56.3.
Definitions	56.4.
Exposure Determination	56.5.
Compliance Methods	56.6.
Supervisory Criminal Investigator's Responsibilities	56.7.
Housekeeping	56.8.
Medical Surveillance Exposure Program	56.9.
Exposure Procedures	56.10.
Warning Labels	56.11.
Training and Information	56.12.
Recordkeeping	56.13.
Compliance Monitoring	56.14.

56.1. Purpose. The purpose of this chapter is to establish an Exposure Control Plan (**Attachment A**) to minimize the risk of Defense Criminal Investigative Service (DCIS) employees being occupationally exposed to the human immunodeficiency virus (HIV) (the virus that causes acquired immune deficiency syndrome (AIDS)), hepatitis B virus (HBV), hepatitis C virus (HCV), syphilis, other bloodborne pathogen diseases, and tuberculosis (TB).

56.2. General. The Department of Labor, Occupational Safety and Health Administration (OSHA), "Bloodborne Pathogens," title 29, Code of Federal Regulations (CFR), section 1910.1030, December 6, 1991, revised July 1, 2009, requires all employers who have one or more employees with occupational exposures to develop and implement a Bloodborne Pathogen (BBP) Exposure Control Plan that establishes responsibility, policy, and procedures for safe handling of biohazard materials and protection of employees from occupational exposure to infectious disease-causing agents. Occupational exposures are any reasonably anticipated skin, eye, mucous membrane, or parenteral contact with blood or other potentially infectious material (see paragraph 56.4.t.) that may result from the performance of an employee's duties.

56.2.a. These preceding and other regulations are intended to save lives, prevent injuries, and protect workers from diseases spread through blood and other potentially infectious materials (OPIM) in contact with unprotected open skin, eye, mucous membranes, or parenteral routes.

56.2.b. Although a variety of harmful microorganisms may be transmitted through contact with infected human blood, HBV, HIV, HCV, and syphilis have been shown to be

responsible for occupationally infecting workers who were exposed to human blood and certain other body fluids through needle stick injuries and by direct contact of mucous membranes, eyes, and non-intact skin with contaminated blood and materials.

56.3. Scope and Applicability. Within DCIS, the Special Agent in Charge, Internal Operations Directorate is responsible for ensuring the BBP and TB Exposure Control Plan meets regulatory and operational requirements, implementing the plan, and maintaining medical and training records in accordance with the directive. The Training/Health and Wellness Program Manager is designated as the BBP/TB Exposure Control Plan Program Manager. Copies of this Plan are to be maintained permanently in obvious and readily accessible locations in all DCIS offices.

56.4. Definitions. See 29 CFR 1910.1030(b).

56.4.a. **Assistant Secretary** means the Assistant Secretary of Labor for Occupational Safety and Health, or designated representative.

56.4.b. **Blood** means human blood, human blood components, and products made from human blood.

56.4.c. **Bloodborne Pathogens (BBP)** means pathogenic microorganisms that are present in human blood and can cause disease in humans. These pathogens include, but are not limited to, hepatitis B virus (HBV) and human immunodeficiency virus (HIV).

56.4.d. **Clinical Laboratory** means a workplace where diagnostic or other screening procedures are performed on blood or other potentially infectious materials.

56.4.e. **Contaminated** means the presence or the reasonably anticipated presence of blood or other potentially infectious materials on an item or surface.

56.4.f. **Contaminated Laundry** means laundry that has been soiled with blood or other potentially infectious materials or may contain sharps.

56.4.g. **Contaminated Sharps** means any contaminated object that can penetrate the skin including, but not limited to, needles, scalpels (knives), broken glass, broken capillary tubes, and exposed ends of dental wires.

56.4.h. **Decontamination** means the use of physical or chemical means to remove, inactivate, or destroy bloodborne pathogens on a surface or item to the point where they are no longer capable of transmitting infectious particles and the surface or item is rendered safe for handling, use, or disposal.

56.4.i. **Director** means the Director of the National Institute for Occupational Safety and Health, U.S. Department of Health and Human Services, or designated representative.

56.4.j. **Engineering Controls** means controls (e.g., sharps disposal containers, self-sheathing needles, safer medical devices such as sharps with engineered sharps injury protections

and needleless systems) that isolate or remove the bloodborne pathogen hazard from the workplace.

56.4.k. **Exposure Incident** means a specific eye, mouth, other mucous membrane, non-intact skin, or parenteral (i.e., taken into the body other than through the digestive tract, such as intravenous injection or knife wound) contact with blood or other potentially infectious material that results from the performance of duties.

56.4.l. **Hand-Washing Facility** means a facility providing an adequate supply of running potable water, soap, and single-use towels or hot-air drying machines.

56.4.m. **HBV** means hepatitis B virus.

56.4.n. **HIV** means human immunodeficiency virus.

56.4.o. **Licensed Healthcare Professional** is a person whose legally permitted scope of practice allows him or her to independently perform the activities required for Hepatitis B vaccination and post-exposure evaluation and followup.

56.4.p. **Needleless Systems** means devices that do not use needles for (1) the collection of bodily fluids or withdrawal of body fluids after initial venous or arterial access is established; (2) the administration of medication or fluids; or (3) any other procedure involving the potential for occupational exposure to bloodborne pathogens due to percutaneous injuries from contaminated sharps.

56.4.q. **Non-Risk Body Fluids** include tears, sweat, saliva, urine, stool, vomitus, nasal secretions, and sputum.

56.4.r. **Occupational Exposure** means reasonably anticipated skin, eye, mucous membrane, or parenteral contact with blood or other potentially infectious material that may result from the performance of an employee's duties.

56.4.s. **Office Supervisor**. In field offices, the Special Agent in Charge (SAC) or a delegated representative. In resident agencies, the Resident Agent in Charge (RAC). In unsupervised offices, the senior special agent. At Headquarters, the SAC or a delegated representative.

56.4.t. **Other Potentially Infectious Materials (OPIM)** means (1) the following human body fluids: semen, vaginal secretions, cerebrospinal fluid, synovial fluid, pleural fluid, pericardial fluid, peritoneal fluid, amniotic fluid, saliva in dental procedures, any body fluid that is visibly contaminated with blood, and all body fluids in situations where it is difficult or impossible to differentiate between body fluids; (2) any unfixed tissue or organ (other than intact skin) from a human (living or dead); (3) HIV-containing cell or tissue cultures, organ cultures, and HIV- or HBV-containing culture medium or other solutions; and (4) blood, organs, or other tissues from experimental animals infected with HIV or HBV.

56.4.u. **Parenteral** means piercing mucous membranes or the skin barrier through such events as needle sticks, human bites, cuts, and abrasions.

56.4.v. **Personal Protective Equipment (PPE)** means specialized clothing or equipment worn by an employee for protection against a hazard. General work clothes (e.g., uniforms, pants, shirts, or blouses) not intended to function as protection against a hazard are not considered to be personal protective equipment.

56.4.w. **Regulated Waste** means liquid or semi-liquid blood, or other potentially infectious materials; contaminated items that would release blood or other potentially infectious materials in a liquid or semi-liquid state if compressed; items that are caked with dried blood or other potentially infectious materials and are capable of releasing these materials during handling or compressing; contaminated sharps; and pathological and microbiological wastes containing blood or other potentially infectious materials. (State regulation applies if equal to or more stringent than Federal OSHA requirements, e.g., California OSHA.)

56.4.x. **Sharps** are any object that can penetrate the skin (e.g., needles, jagged glass, knives).

56.4.y. **Sharps with Engineered Sharps Injury Protections** means a non-needle sharp or a needle device used for withdrawing body fluids, accessing a vein or artery, or administering medications or other fluids, with a built-in safety feature or mechanism that effectively reduces the risk of an exposure incident.

56.4.z. **Source Individual** means any individual, living or dead, whose blood or other potentially infectious materials may be a source of occupational exposure to the employee. Examples include, but are not limited to, hospital and clinic patients; clients in institutions for the developmentally disabled; trauma victims; clients of drug and alcohol treatment facilities; residents of hospices and nursing homes; human remains; and individuals who donate or sell blood or blood components. Source individual also includes arrested persons and gunshot victims.

56.4.aa. **Sterilize** means the use of a physical or chemical procedure to destroy all microbial life including highly resistant bacterial endospores.

56.4.ab. **Tuberculosis (TB)** is a common infectious disease caused by various strains of *Mycobacterium tuberculosis* in humans. It is usually spread through the air when a person with TB of the lungs or throat coughs, sneezes, or talks. Most often it attacks the lungs but can also affect other parts of the body. Most infections in humans have no symptoms with the latent infection. About one in ten latent infections eventually progress to active disease, which, if left untreated, kills more than 50 percent of its victims.

56.4.ac. **Universal Precautions** is an approach to infection control. According to the concept of Universal Precautions, all human blood and certain human body fluids are treated as if known to be infectious for HIV, HBV, and other bloodborne pathogens. Body fluids that generally do NOT meet the bloodborne pathogen definition and do not generally fall under the

Universal Precaution requirement are: feces, nasal secretions, urine, vomit, perspiration, sputum, and saliva, unless they contain blood or other human body fluids that do meet the definition.

56.4.ad. **Work Practice Controls** means controls that reduce the likelihood of exposure by altering the manner in which a task is performed (e.g., prohibiting recapping needles by a two-handed technique).

56.5. Exposure Determination

56.5.a. This Plan covers all DCIS employees whose job duties present a potential occupational exposure to blood or other potentially infectious materials as defined in section 56.4. above.

56.5.b. Job classifications will be reviewed and updated annually and as necessary to reflect new or modified tasks and procedures that affect occupational exposures or positions.

56.5.c. The Plan covers GS-1811 Criminal Investigators and GS-1801 Investigative Assistants/Analysts who assist criminal investigators in investigative activities. This classification is covered under this Plan because of the possibility of occupational exposure during the following tasks:

56.5.c.(1). arrests and searches pursuant to arrests;

56.5.c.(2). execution of search and seizure warrants;

56.5.c.(3). interviews involving potentially hostile individuals;

56.5.c.(4). escorting prisoners;

56.5.c.(5). evidence handling and other law enforcement activities in connection with criminal, civil, and administrative investigations.

56.6. Compliance Methods

(b)(7)(E)

CHAPTER 58

HEALTH AND WELLNESS PROGRAM

<u>Contents</u>	<u>Section</u>
General	58.1.
Program Management	58.2.
Program Description	58.3.
Medical Evaluation Program	58.4.
Medical Records—Employee Medical File System	58.5.
Physical Readiness Test (PRT)	58.6.
Pre-Employment Physical Readiness Test	58.7.
PRT Program Evaluation	58.8.
Health and Wellness Assessments	58.9.
Regular Fitness Maintenance/Improvement Activity	58.10.
Confidentiality—Physical Readiness Test	58.11.

58.1. General

58.1.a. This chapter outlines the policies and procedures relating to the Health and Wellness Program for **all** GS series 1811 criminal investigators (i.e., special agents) of the Office of the Inspector General of the Department of Defense (OIG DoD). This includes members of the Senior Executive Service (SES) who are criminal investigators.

58.1.b. The goals of this program are to improve the health and wellness of special agents and their performance of criminal investigative duties, ensure safety in the performance of such duties, and promote a professional law enforcement image.

58.1.c. Occasions will arise when special agents must be prepared to perform law enforcement tasks that require arduous physical exertion, such as pursuing and subduing hostile persons. This requires the criminal investigator to be physically fit in the categories of strength, flexibility, and cardiovascular endurance. It also requires that the criminal investigator maintain a state of wellness that includes a combination of exercise, good nutrition, and rest to prevent debilitating disease.

58.1.d. Extended and irregular work hours are inherent in the criminal investigator position and require that special agents maintain physical fitness.

58.1.e. Special agents are representatives of a professional law enforcement organization and, as such, must at all times project a professional Federal law enforcement image. Such an image demands physical conditioning. Every person who accepts a position as a criminal investigator accepts the responsibility to maintain that image.

58.1.f. All special agents should recognize their responsibility to maintain the physical conditioning necessary for them to exercise their duty as Federal law enforcement officers.

58.1.g. Criminal investigator fitness will not only result in a more productive and professional workforce, it will physically and psychologically benefit every participating special agent.

58.1.h. To better comprehend the DCIS Health and Wellness Program, it is necessary to understand the distinction between “wellness” and “fitness.” Wellness pertains to an individual’s health and disease status and the risk potential for contracting disease as well as overall positive well-being. Physical fitness pertains to an individual’s ability to use his/her body and mind in activities requiring strength, muscular endurance, cardiorespiratory fitness, flexibility, coordination, agility, power, balance, and speed – without undue fatigue and exhaustion.

58.2. Program Management

58.2.a. The DCIS Health and Wellness National Program Manager (NPM) assigned to the Internal Operations Directorate (IOD) will manage the overall program. The NPM’s responsibilities include the following.

58.2.a.(1). Supervise the collection of semiannual Physical Readiness Test (PRT) data and the statistical analysis of it for all OIG DoD criminal investigators.

58.2.a.(2). Coordinate the staffing and training of all field and Headquarters (HQ) Health and Wellness Coordinators/Instructors.

58.2.a.(3). Serve as the focal point for coordinators/instructors in program administrative matters.

58.2.a.(4). Stay abreast of scientific research and studies that pertain to fitness/wellness issues and make that information available to special agents through a system that involves input from all DCIS Health and Wellness Coordinators, including the development and dissemination of wellness and fitness educational materials.

58.2.a.(5). Maintain communication and act in concert with Federal Occupational Health (FOH) to assist in the delivery of proper annual medical examinations.

58.2.a.(6). Maintain all FOH medical exam forms and medical waivers regarding all OIG DoD criminal investigators.

58.2.a.(7). Respond to technical questions that arise from the annual physicals and, when necessary, direct the criminal investigator to medical authorities for resolution. The NPM is responsible for coordinating the medical review process, assembling medical documentation and appeals, and corresponding with the OIG DoD Medical Review Board (MRB), OIG DoD representatives, and the employee.

58.2.a.(8). Maintain a program of continuing education to ensure current certification status of Health and Wellness Coordinators/Instructors. The goal of maintaining “current certifications” will be for the Health and Wellness Coordinators to participate in refresher training every 5 years, as well as identifying training opportunities throughout the year.

58.2.a.(9). Maintain liaison with the Federal Law Enforcement Training Center (FLETC) Physical Techniques Division, noted authorities and experts in the field of health and physical fitness, as well as colleges and universities to ensure that the best possible program is maintained and updated.

58.2.a.(10). Ensure that all OIG DoD criminal investigators are familiar with the DCIS Health and Wellness Program and the components of the PRT to establish the fundamentals for a career of health and wellness maintenance.

58.2.a.(11). Host a training program for field office Coordinators to review the program’s viability and make changes or improvements when needed.

58.2.a.(12). In conjunction with the Health and Wellness Instructors, develop informational packages for all instructors to use with the PRT.

58.2.a.(13). Develop and distribute a periodic e-mail, with input and recommendations from the Health and Wellness Instructors, providing information regarding health and fitness.

58.2.a.(14). Consistent with available resources, develop a block of training to present at the DCIS Special Agent Basic Training Program (SABT) and the Special Agent Refresher Training Program (SARTP) dealing with fitness, health, general wellness, and Program management.

58.2.a.(15). Provide a statistical overview of the Program on an annual basis to all supervisory levels. The overview should include information pertaining to criminal investigator use of the 4 hours per week authorized physical training (PT) time and summary PRT scoring. Statistics from previous years will be provided for comparison purposes and the information will be generic, with no individual special agents being identified.

58.2.b. The Program will be coordinated at the field office level by a field office Health and Wellness Coordinator, who will be selected by the Special Agent in Charge (SAC) to perform in that capacity as a collateral duty. The field office Health and Wellness Coordinator’s responsibilities will include the following (in addition to the responsibilities of a Health and Wellness Instructor).

58.2.b.(1). Supervise the collection of semiannual PRT data and certify that all special agents complete an annual assessment for their respective field office and ensure that it is forwarded to the NPM by the required reporting dates.

58.2.b.(2). Provide the number, availability, and status of instructors within the field office to the SAC and Assistant Special Agent in Charge (ASAC) in an annual Field Office Program Profile, with a copy to the NPM, by May 30. The Field Office Program Profile will also include award recommendations, the status of first aid/cardiopulmonary resuscitation (CPR) certifications, Health and Wellness Instructor certifications/training, and a short summary of Program status and recommendations. See Attachment A for the reporting requirements and format.

58.2.b.(3). Notify the NPM, via memorandum, of any medical waivers from the PRT within their respective field office.

58.2.b.(4). Ensure that all criminal investigators within their respective field office are familiar with the DCIS Health and Wellness Program.

58.2.b.(5). Take responsibility for conducting voluntary health and wellness assessments.

58.2.b.(6). Provide feedback on the Program to include the PRT and annual assessments, as well as recommended improvements for the wellness portion of the Program. Incorporate this feedback into the Field Office Program Profile.

58.2.c. All Health and Wellness Instructors will be responsible for the following duties and possess the following qualifications.

58.2.c.(1). Maintain a thorough knowledge and strict adherence to all policy and requirements of Special Agents Manual (SAM) Chapter 58, "Health and Wellness Program."

58.2.c.(2). Maintain current certification in basic first aid and CPR. This training and recertification should be obtained from local sources (e.g., American Red Cross, fire departments, and military). Make a reasonable effort to obtain this training free of charge. If payment is required before attending the training, an SF 182 (Authorization Agreement Certification of Training) must be completed and approved in advance by the immediate supervisor and the DCIS Headquarters Training Coordinator.

58.2.c.(3). Determine the health and fitness needs of individual criminal investigators through annual assessments.

58.2.c.(4). Administer the semiannual PRT.

58.2.c.(5). Provide health and fitness instruction in conjunction with the PRT using briefing packages provided by the NPM.

58.2.c.(6). Be an advocate of the Program and possess an interest in health and wellness.

58.2.c.(7). Be able to pass the FLETC Law Enforcement Fitness Coordinator Training Program, which includes passing the FLETC Physical Efficiency Battery at the 40th percentile.

58.2.c.(8). Have no long-term disability that would prevent the instructor from participating in all components of the DCIS PRT.

58.2.d. Health and Wellness Instructors are encouraged to provide information, articles, results of studies, and pertinent Web sites to the NPM for compilation into a periodic e-mail for the Office of the Deputy Inspector General for Investigations.

58.3. Program Description. The Health and Wellness Program consists of the following elements:

58.3.a. a medical evaluation program conducted by FOH,

58.3.b. the OIG DoD MRB,

58.3.c. semiannual PRT,

58.3.d. voluntary annual Health and Wellness assessment conducted by a DCIS Health and Wellness Instructor,

58.3.e. Voluntary on-duty and off-duty fitness maintenance/improvement activity (PT).

58.4. Medical Evaluation Program

58.4.a. **Medical Examination.** All 1811 criminal investigators (i.e., special agents) with the OIG DoD will undergo an FOH medical examination every other year. Complete exams consist of an initial visit with the FOH nurse followed by a second visit with the FOH medical doctor. This “complete” medical examination will include the following.

58.4.a.(1). **Required Services**

58.4.a.(1).(a). General Physical Exam

58.4.a.(1).(b). General Medical History

58.4.a.(1).(c). Vision Screening (corrected or uncorrected, near and far, peripheral, depth perception, and use of Ishihara 14 plate edition to assess color)

58.4.a.(1).(d). Audiometry

58.4.a.(1).(e). DFOH Profile (blood and urine)

58.4.a.(1).(f). EKG

58.4.a.(1).(g). Prostate Specific Antigen (for male special agents 40 years of age and older)

58.4.a.(1).(h). Cervical cancer screening (for female special agents 40 years of age and older)

58.4.a.(1).(i). Tetanus inoculation (every 10 years)

58.4.a.(2). **If Indicated Services.** These services are to be performed if the FOH Medical Review Officer (MRO) has determined that further testing is medically warranted.

58.4.a.(2).(a). Stool Occult Blood

58.4.a.(2).(b). Cardiovascular Stress Test (with DCIS approval)

58.4.a.(2).(c). TB-Mantoux PPD

58.4.a.(2).(d). Chest X-ray

58.4.a.(2).(e). Lead, Blood, and APP (firearms instructors only)

58.4.a.(2).(f). Pyrometer

58.4.b. **Reporting Requirements.** When required to complete a medical exam, both parts of the exam must be scheduled and completed within the time period specified by the NPM (generally no later than May 30). All DCIS field office SACs are required to send an e-mail to the Assistant Inspector General for Investigations (AIGI) for Investigative Operations (IO) and the NPM certifying that all agents up to the GS-15 level have met this requirement. Any agents who have not met this requirement will be identified in the e-mail along with an explanation as to why they have been unable to schedule their appointment(s). Responsibility for DCIS HQ compliance will be handled by the appropriate HQ AIGI and their respective Deputy AIGI. The NPM is responsible for collating all delinquencies and forwarding them through the chain of command to the Deputy Inspector General for Investigations (DIGI). All DCIS agents who are members of the SES must certify through an e-mail to the DIGI, with a cc to the NPM, that they have met this requirement. All other OIG SES criminal investigators, to include the DIGI (if applicable) are required to certify and e-mail the Principal Deputy Inspector General (PDIG), with a copy to the NPM, that they have met this requirement.

58.4.c. **Results of Medical Examination.** The FOH MRO will report to the NPM whether a criminal investigator has met the OIG DoD medical qualification standards. The specific medical qualification standards for OIG DoD 1811 criminal investigator positions are listed in Attachment B. If a criminal investigator does not meet the OIG DoD medical qualifications standards, the FOH MRO will recommend followup medical testing. The OIG DoD will pay up to \$300 per fiscal year for the cost of the office visits and associated testing to

diagnose the condition. Subsequent medical treatment (and its associated costs) for any diagnosis is the responsibility of the special agent.

58.4.d. Deferred Medical Determination. In some instances, the FOH MRO may defer making a medical determination pending receipt of followup medical exam information from a special agent. In such instances, the special agent's medical status will be listed as pending. It is the special agent's responsibility to ensure all followup medical exams have been scheduled within 30 days from the date of receipt of the medical review form. Agents are required to document the dates of their medical followup exams by an e-mail notification to the NPM. Although agents are responsible for ensuring all medical followup information is received by the FOH MRO, agents will not be penalized for any delay caused by a healthcare provider or FOH, so long as the agent can show they made reasonable efforts to obtain the information from the physician. In those instances where the 30-day time limit cannot be met, the criminal investigator must request an extension through their supervisor to the NPM detailing the reasons why an appointment could not have been scheduled during the initial timeframe. The NPM may approve the extension for up to an additional 60 days. All DCIS criminal investigators at the GS-15 level and below who fail to schedule their initial medical followup appointment within the approved extension must submit a request for additional time through their chain of command to the appropriate AIG with a carbon copy (cc) to the NPM. The request must include detailed reasons for failing to schedule the appointment within the previously granted extension and provide an estimate of when the followup appointment can be scheduled. Based on the criminal investigator's request, the AIG may grant an additional extension. Additionally, depending on the nature of the details in the request, the AIG may suspend the criminal investigator's authorized 4 hours of official on-duty exercise time pending completion of the examination. The criminal investigator's performance evaluation may also be negatively impacted. INV AIGs will forward their requests for extension to the DIGI. All other OIG GS-15 and below criminal investigators will request an extension from their respective component head. All other OIG SES criminal investigators must submit their requests to the PDIG. All requests must be sent with a cc to the NPM.

58.4.d.(1). In those instances where an OIG criminal investigator has completed his/her medical followup visit, but the medical provider has failed to forward the documentation to the MRO, the NPM will coordinate with the MRO and attempt to schedule a teleconference with the criminal investigator's healthcare provider to resolve the situation.

58.4.d.(2). All OIG criminal investigators whose medical status is listed as pending after the 60-day extension because he/she has not completely recovered from a medical condition will be required to request a medical waiver or a reasonable accommodation. DCIS criminal investigators will submit their request to the respective AIGs. All other OIG GS-15 and below special agents will submit their requests to the respective component head. INV AIGs will forward their requests for extension to the DIGI; all other OIG SES special agents must submit their requests to the PDIG. All requests must be sent with a cc to the NPM. Medical waiver decisions or reasonable accommodation requests must be renewed after 365 days from the date of the memorandum. If an agent's medical status is still pending upon expiration of the initial medical waiver or reasonable accommodation, the agent's condition will be referred to the

OIG MRB to determine whether the employee requires an additional waiver, reassignment, or consideration for medical retirement.

58.4.e. Fitness for Duty. After consultation with Human Capital Advisory Services (HCAS) and the OIG DoD Office of General Counsel (OGC), a supervisor may request that a criminal investigator be medically and/or psychologically examined/evaluated at any time that concerns arise regarding the special agent's ability to perform the physical and mental requirements of the job. Concerns over personality and emotional disorders can also be included in requests for fitness for duty examinations/evaluations. DCIS supervisors must first obtain the approval of the appropriate AIG before referring a criminal investigator at the GS-15 level or below to the NPM to initiate the fit for duty process. All DCIS SES criminal investigators fit for duty requests will be submitted to the DIGI. All other OIG SES criminal investigators, to include the DIGI if applicable, fit for duty requests will be submitted to the PDIG. The NPM in coordination with the FOH, OGC, HCAS, and the appropriate chain of command will facilitate the fit for duty process.

58.4.f. Change in Medical Condition. A criminal investigator is responsible for informing his/her immediate supervisor whenever any change in his/her medical condition, including the use of medication, could affect the performance of his/her duties.

58.4.g. Medical Disqualifications

58.4.g.(1). If the FOH MRO determines that a criminal investigator does not meet the OIG DoD medical qualifications standards for 1811 criminal investigators, other evaluative tests may be required. Such tests will be based upon the recommendation of the FOH MRO or the special agent's personal physician, as applicable.

58.4.g.(2). Medical evaluation recommendations are initially made by the FOH MRO and then forwarded to the NPM. Upon notice that a criminal investigator is not medically qualified to perform the essential functions of the job, OIG DoD management must immediately relieve the employee of hazardous and/or rigorous duties. Hazardous duties are defined as those that are so dangerous or physically demanding that an incumbent's medical condition becomes a necessary and important consideration in determining his or her ability to perform safely and efficiently. Rigorous duties include mental or physical activities that are so strenuous that they require the establishment of age limits and physical performance standards.

58.4.h. Appeal of Medical Disqualifications. OIG criminal investigators may appeal disqualification determinations by submitting a request to the DoD OIG MRB for a medical waiver, reasonable accommodation, or a second opinion through their chain of command to the NPM within 30 calendar days of receiving notice that they did not meet the medical qualifications standards. The DoD OIG MRB will be responsible for reviewing an applicant or incumbent's medical evaluation that disqualifies them from the 1811 criminal investigator position. The MRB will consist of three voting members. For all criminal investigators at the GS-15 level or below, the voting members will be the three INV AIGs. For all SES criminal investigators, the MRB voting members will consist of the PDIG, the OIG Chief of Staff, and the AIG for Administration and Management. The MRB will consist of the following advisory

members: NPM, MRO, OIG OGC, and a member from the OIG HCAS. All members of the MRB will consider the written record of all evaluations and any written or oral submission presented by the employee before making a decision on the employee's request. In order to reduce costs, oral presentations will be made typically by teleconference or videoconference no sooner than 5 working days after the submission of all medical records and written correspondence. The MRB will convene only when a quorum of, or at a minimum, the NPM and all three voting members are present.

58.4.i. Medical Waivers. Since medical conditions may improve, deteriorate, or resolve, criminal investigators may request a medical waiver from the MRB. Should the employee's medical condition deteriorate, the employee must apply for a renewal of the waiver. All waivers must be renewed on an annual basis. Attachment C is a sample of a Waiver Request. Attachment D is a sample Medical Standards Waiver Decision Memorandum, and Attachment E is a sample Waiver Renewal.

58.4.j. Reasonable Accommodation. Accommodations may be considered where there is sufficient evidence to establish that the disqualified criminal investigator is or could be a qualified individual with a disability. The request must be initiated by the employee. A qualified individual with a disability is someone who satisfies skill, experience, education, and other job-related requirements of the position and who, with or without reasonable accommodation, can perform the essential functions of the position without endangering the health and safety of themselves or others with or without the requested accommodation. All requests for reasonable accommodations must be coordinated through the OIG Equal Employment Opportunity Office (EEO). If there is sufficient evidence to establish that the criminal investigator is a qualified individual with a disability, then the MRB will review the request for consideration. The MRB will render a written decision to the criminal investigator through the appropriate chain of command. Since medical conditions may improve, deteriorate, or resolve, all approved reasonable accommodation requests must be renewed on an annual basis. OIG DoD shall make reasonable accommodation to known physical or mental limitations of a criminal investigator who is a qualified individual with a disability, unless it can be demonstrated that the accommodation would impose an undue hardship on program operations. Reasonable accommodation may include, but shall not be limited to, making facilities readily accessible to, and usable by, individuals with disabilities; job restructuring; part-time or modified work schedules; acquisition or modification of equipment or devices; and appropriate adjustment or modification of examinations. In determining whether an accommodation would impose an undue hardship on the operation of the OIG DoD, consider the following factors: the overall size of the program/office with respect to the number of employees; number and type of facilities and size of budget; the type of program/office operation, including the composition and structure of the workforce; and the nature and cost of the accommodation. Consultation with the OIG EEO Office is required in making this evaluation.

58.4.k. Second Opinions

58.4.k.(1). If the criminal investigator is medically disqualified based upon the results of a medical examination, he/she can request another examination. The second examination will be limited to the area of concern that led to the unacceptable finding in the earlier examination. It may be conducted either by a physician mutually acceptable to the OIG

DoD and the criminal investigator, or by a physician chosen by the criminal investigator. If a mutually acceptable physician is used, costs for further medical examination up to \$300 per fiscal year are the responsibility of the OIG DoD. If the criminal investigator elects to use a physician of his or her choice (i.e., a physician not acceptable to the OIG DoD due to qualifications, cost, distance, or time considerations), the examination will be conducted on the criminal investigator's time and at his or her own expense. During the period prior to this second examination, the employee will be in a non-duty (administrative leave) status, or will be assigned light duty.

58.4.k.(2). If after the second medical examination, the FOH MRO makes a determination that no further medical testing, referrals to specialists, expert consultations, and other diagnostic techniques are required, the criminal investigator is responsible for any further testing. The criminal investigator must submit the results of the second examination for review and recommendation to the FOH MRO. The FOH MRO's subsequent recommendation will be submitted to the OIG MRB. The employee has 60 calendar days from his or her receipt of the notice of failure to meet the medical qualification standards to provide this information to the agency. However, during the period of reconsideration, the employee will be in a non-duty (administrative leave) status, or will be assigned light duty.

58.4.l. Actions Subsequent to Confirmed Disqualifications. In the event a criminal investigator has exhausted all avenues of appeals and it is still determined that he/she cannot perform the essential functions of the position for at least 365 days from the original date of the medical disqualification, he or she is disqualified from holding a rigorous and/or hazardous duty position. It is OIG DoD policy to take appropriate action to remove the disqualified criminal investigator from the position in the least punitive manner. Appropriate action will be considered in the following order.

58.4.l.(1). **Reassignment.** An employee who is physically disqualified for his/her former position due to a compensable injury is entitled, within 1 year of the date he/she began receiving compensation, to be placed in a position for which he/she is qualified that most closely approximates the seniority, status, and pay to which the employee would otherwise have been entitled (5 CFR 353.301(c)). In the absence of available positions at the same grade level, the criminal investigator may be offered a position at the highest available grade level below the one he or she currently occupies.

58.4.l.(2). **Disability Retirement.** The Defense Finance and Accounting Service, Regional Service Center (DFAS RSC), and the OIG HCAS provide benefits counseling/services for the OIG DoD. DFAS RSC and the OIG HCAS will determine upon request from the criminal investigator whether he or she is eligible for disability retirement. A DFAS RSC Benefits Specialist will provide counseling to a criminal investigator eligible for disability retirement for all non-worker's compensation disability benefits. The OIG Injury Compensation Program Administrator provides counseling for disability retirement only when the disability is due to a compensable (work-related) injury. An employee is eligible for disability retirement only if:

58.4.l.(2).(a). the disabling medical condition is expected to continue for at least 1 year;

58.4.l.(2).(b). the condition results in a deficiency in performance, conduct, or attendance, or is incompatible with useful and efficient service or retention in the employee's position; and

58.4.l.(2).(c). the agency is unable to accommodate the disabling condition in the employee's position or in an existing vacant position. See 5 CFR 831.1203; *Bracey v. Office of Personnel Management*, 236 F.3d 1356, 1358 (Fed. Cir. 2001).

58.4.l.(3). **Removal.** In the event there are no vacant positions to which the criminal investigator can be reassigned, and he or she is not eligible for disability retirement or elects not to apply, OIG DoD management may initiate action to remove him or her from Federal service.

58.4.m. **Eligibility for Rehire.** A criminal investigator is entitled to be restored immediately and unconditionally to his/her former position, or an equivalent one, if he/she recovers from a compensable injury within 1 year of the date he/she began receiving compensation (5 CFR 353.301(a)). If a criminal investigator has been removed for more than 1 year, he/she may reapply for a criminal investigator position if the OIG has a vacancy and if further medical evaluations, treatment, and/or testing conducted by medical professionals result in a medical conclusion by the FOH MRO that the condition does not exist or is no longer disqualifying. The applicant must be capable of safely performing all duties of the criminal investigator position and meet all other training and eligibility criteria.

58.4.n. **Payment Procedures.** The OIG DoD authorizes reimbursement of medical-related expenses as the result of followup information ordered or offered by the FOH. Any exam the applicant or employee takes on their own initiative will be at their personal expense and not subject to reimbursement.

58.4.n.(1). Make claims for reimbursement only through an SF 1164, "Claim for Reimbursement for Expenditures on Official Business." The SF 1164 must be accompanied by proof of payment.

58.4.n.(1).(a). The criminal investigator will complete and submit the SF 1164 and proof of payment to the Approving Official.

58.4.n.(1).(b). The Approving Official, who is the Deputy AIGI, IOD, will:

58.4.n.(1).(b).1. review the SF 1164 with proof of payment and determine whether the expenses listed are within the area of concern recommended by the FOH MRO for medical examination followup;

58.4.n.(1).(b).2. ensure that the following statement is on the form with the Approving Official's initials and date, "The claimant did not meet the medical standards and requirements of his/her position; therefore, the medical expenses on this form are proper for payment"; and

58.4.n.(1).(b).3. approve the SF 1164 in Block 8 and forward the approved form and proof of payment to the Comptroller.

58.4.n.(1).(c). The Comptroller will:

58.4.n.(1).(c).1. verify the completion of the SF 1164, the cost of the reimbursements, and the receipt providing proof of payment;

58.4.n.(1).(c).2. provide an accounting classification for the approved SF 1164; and

58.4.n.(1).(c).3. certify the SF 1164 in Block 9 and forward it to the Defense Finance and Accounting Service-Indianapolis for payment.

58.4.n.(2). All claims for local travel (parking expenses and local mileage) incurred while undergoing agency-directed medical evaluations will be paid with local travel funds and according to standard agency procedures. All local travel expenses are reimbursed through the Defense Travel System.

58.5. Medical Records—Employee Medical File System

58.5.a. FOH maintains original medical exam information in accordance with the provisions of the Privacy Act of 1974 and Health Insurance Portability and Accountability Act of 1996 (HIPAA). The FOH MRO reports to the NPM and/or the Program Director for Training whether a criminal investigator has met OIG DoD medical qualification standards. The NPM is responsible for maintaining these reports and any other records generated because of an employee's medical condition in a manner that strictly controls access to the information and assures the safety and integrity of these records.

58.5.b. The OIG DoD will maintain employee medical files for the period of the employee's service with the OIG DoD, and then transfer the files to the National Personnel Records Center for storage within 30 days of separation. The NPM is responsible for reviewing OIG DoD files and coordinating with FOH to determine if any records need to be archived in accordance with this chapter.

58.5.c. Employees must be provided access to their medical records. This access must be prompt (generally within 15 working days) and present no unreasonable barriers for the employee.

58.5.d. Without a signed consent from the subject employee, no confidential information will be released to or shared with individuals other than:

58.5.d.(1). authorized FOH officials or contracted health professionals who work as representatives of the OIG DoD and have a justified programmatic need to know;

58.5.d.(2). other individuals within the OIG DoD with a specific official need to know, to include those summarized in section 58.4.; and

58.5.d.(3). authorized Occupational Safety and Health Administration (OSHA) and Office of Personnel Management (OPM) officials.

58.6. Physical Readiness Test (PRT)

58.6.a. The PRT will be administered semiannually (spring and fall) in one continuous session. All special agents who have been medically cleared by the FOH MRO are required to participate in the PRT as a duty associated with their position as criminal investigators. Any criminal investigator who has a medical restriction is not authorized to take the PRT. Prior to participation in the PRT, the special agent will be required to complete the DCIS Health Screening Questionnaire (Attachment F) and provide a copy to the local Health and Wellness Instructor. The purpose of the questionnaire is to identify individuals who may be at risk in taking the DCIS PRT and recommend a medical examination prior to taking the PRT. It is the special agent's responsibility to notify and update management on the status of any medical restrictions. Special agents must complete a makeup PRT within 10 working days after a medical restriction has been lifted.

58.6.b. Only Health and Wellness Instructors trained and certified by FLETC or an alternate certifying entity (i.e., Cooper Institute) approved by the Deputy AIGI IOD will conduct physical readiness testing.

58.6.c. The PRT is a "constructive physical fitness test," which means that although it does not measure a special agent's ability to perform specific criminal investigator tasks, it is a reliable predictor of how well a criminal investigator will be able to perform the physically demanding duties common to law enforcement. The test is based upon The Cooper Institute, Dallas, TX, fitness assessment protocol.

58.6.d. The PRT measures the special agent's fitness in the areas of cardiovascular endurance, flexibility, and strength by using age and gender norms established by The Cooper Institute. The Cooper age and gender norms represent how individuals in a specific age and gender group compare to one another with regard to physical fitness performance.

58.6.e. The SACs may excuse special agents at the GS-14 level and below from the PRT for special operational needs or exceptional circumstances (e.g., previously scheduled leave, non/optional temporary duty, other scheduled training). The SACs must notify the NPM, via e-mail, of the excuse. The AIGI IOD may excuse SACs, but must notify the NPM via e-mail. The DIGI may excuse all DCIS SES special agents. All other OIG special agents at the GS-15 level or below must receive approval from their component head with notification to the NPM. All other OIG SES special agents must receive approval from the PDIG to be excused, with notification forwarded to the NPM. Only one absence within a year will be approved. Any exceptional circumstance that results in more than one absence will be coordinated with the

NPM. The Health and Wellness Instructor will document the absence in the Annual Field Office Program Profile (Attachment A). Special agents who fail to take the scheduled PRT or makeup test may lose the authorized 4 hours of on-duty PT time per week. The special agent's immediate supervisor, in consultation with the appropriate chain of command, will make this decision.

58.6.f. It is the special agent's responsibility to notify and update management and the Health and Wellness Instructor of any temporary or chronic medical condition that may affect the special agent's successful and safe participation in the PRT or PT. Such notification should be made within 48 hours of the condition's onset.

58.6.g. Special agents may be excused from portions of the PRT due to temporary or chronic medical/physical conditions. Such excuse is only temporary and the agent must fulfill the requirement within 10 working days of the restriction being lifted.

58.6.g.(1). The Health and Wellness Instructor may excuse special agents with temporary medical/physical conditions (e.g., sprain, influenza) from the PRT until the condition no longer exists, at which time the Health and Wellness Instructor will schedule a makeup test within 10 working days.

58.6.g.(2). Women who are pregnant must have a physician's approval before any fitness testing. Women in the first two trimesters may elect to test, but will not be required. Testing is discouraged during this time, but not prohibited. Women in their third trimester will not be permitted to test.

58.6.g.(3). Special agents with chronic (i.e., of long duration, continuing) medical/physical conditions may defer testing if they are under medical care for a condition that would affect test results. A written waiver from a licensed physician is required. The waiver must contain a statement from the physician detailing the special agent's medical condition that prohibits him/her from participating in the specific elements of the PRT and for how long. The criminal investigator must forward a copy of the waiver to his or her immediate supervisor as well as to the NPM. The local Health and Wellness Instructor will be notified only that a waiver exists.

58.6.h. The complete PRT protocol is included as Attachment G. Briefly, the test consists of the following elements.

58.6.h.(1). **Pretest Planning and Considerations.** The Health and Wellness Instructor should review CPR techniques and have a plan of action (e.g., ready-access telephone, first aid kit, and location of nearest hospital) in the event of a medical emergency. Ice should be available for first aid.

58.6.h.(2). **Warmup and Stretching Period (required).** Prior to performing the assessments, warmup and stretching activities will be performed. These activities will include light calisthenics, stretching, and other low-intensity activities as recommended by the Cooper

Institute and/or FLETC. The purpose of the warmup is to provide a mild stimulus to the muscle groups that will be used during the remainder of the assessment, thereby reducing the risk of injury.

58.6.h.(3). **Sit and Reach Flexibility (Trunk Flexion) Test.** The measurement of how far the criminal investigator can reach toward or beyond his/her feet from the floor in a seated, legs-extended position.

58.6.h.(4). **Muscular Strength and Endurance**

58.6.h.(4).(a). **Sit-up (Trunk Strength) Test.** The measurement of a special agent's abdominal strength, lower back strength, and muscular endurance through the maximum number of sit-ups in 1 minute.

58.6.h.(4).(b). **Push-up Test.** The measurement of muscular endurance of the upper body (anterior deltoid, pectoralis major, triceps) in 1 minute.

58.6.h.(5). **Cardiovascular Endurance Test.** The measurement of the time it takes the criminal investigator to travel running a distance of 1.5 miles. A criminal investigator may elect to take the alternate cardiovascular endurance test, a 3-mile walk.

58.6.i. Special agents should perform in the PRT to the best of their ability, and strive to score at least in the "fair" fitness category for their age and gender. However, the objective of this program is safe and steady improvement in the physical condition of special agents. Special agents should employ sound judgment and common sense in determining the degree of exertion to which they subject themselves. Those who feel they cannot safely exert themselves to maximum levels should scale down their efforts to remain within the limits of safety. For example, those who feel they cannot safely run or jog the 1.5 miles of the cardiovascular endurance course should walk part or all of the distance. Attachment H is a complete listing of the Cooper age and gender norms.

58.7. Pre-Employment Physical Readiness Test. Appointees are required to take and score in at least the minimum "fair" level in each fitness assessment as a condition of employment. Attachment H (Cooper Age and Gender Norms) sets forth the scores necessary to achieve the fair level in each fitness assessment. All job announcements will include the statement that appointees are required to take and score in at least the minimum "fair" level in each fitness assessment as a condition of their employment offer. The standards will be made available on the DCIS Web site under the Health and Wellness link. A copy of the DCIS PRT age and gender norms will be furnished to all individuals who are interviewed for the criminal investigator position.

58.8. PRT Program Evaluation

58.8.a. Health and Wellness Instructors will notify each criminal investigator of their raw scores (e.g., actual number of push-ups) and the fitness levels achieved in each event. The

information contained therein will be treated confidentially by instructors and furnished only to the special agent, their chain of command, the field office Health and Wellness Coordinator, and the NPM.

58.8.b. The primary field office Health and Wellness Coordinator/Instructor will be responsible for ensuring that all scores have been entered into the physical readiness module of the Investigative Data System (IDS)/CRIMS within 30 days after completion of the scheduled PRT, but no later than May 30 for the spring PRT and November 30 for the fall PRT.

58.9. Health and Wellness Assessments

58.9.a. Healthy lifestyle patterns incorporating a balanced program of exercise, rest, nutrition, and risk management are important preventive measures in the fight against disease, injury, and disability. Beginning and maintaining a health and wellness program is critical for an OIG DoD criminal investigator. Mentally and physically fit, healthy special agents are better equipped to handle the daily stresses of the profession. They have a markedly increased chance of performing well under duress and coping with, and surviving, the physical, mental, and emotional challenges inherent in the profession.

58.9.b. DCIS endorses health and fitness primarily by focusing on the well-being of special agents, but also recognizes the operational and business value of a healthy, physically fit workforce. DCIS encourages individuals to seek the means to achieve and maintain healthy vigorous lives, both on and off the job. In keeping with this philosophy, instructors are required to offer support and helpful encouragement to all special agents through a voluntary health and wellness assessment. A sample assessment checklist is found at Attachment I. At a minimum, the assessment session should provide special agents with a sense of their fitness level, overall health, and how their lifestyle may be affecting their health and wellness. The assessment will consist of the following:

58.9.b.(1). a review of the employee's PRT scores to assist in identifying those areas of fitness that need improvement and fitness level scores over a period. The results will be used for goal setting that will form the basis of a structured program for special agents who want to improve their fitness levels. Fitness plans, to include flexibility, aerobic, and strength training, will be provided to the criminal investigator upon request;

58.9.b.(2). use of assessment materials assembled by the NPM with recommendations and input from the Health and Wellness Instructors. The assessment materials will be developed to provide exercise and nutrition guidance, including goal-setting, motivation, and exercise adherence. The assessment(s) will also address lifestyle issues such as stress and disease avoidance;

58.9.b.(3). stress management techniques;

58.9.b.(4). criminal investigator weight and optional body composition measurements as a record of the special agent's weight management;

58.9.b.(5). optional blood pressure reading. The criminal investigator may also provide his/her blood pressure readings from the most recent physical exam.

58.9.c. The NPM in conjunction with the Health and Wellness Instructors will develop materials to use for assessments and for instruction during the semiannual PRT. One of the goals of Health and Wellness Coordinators Training Seminars will be to assemble an assessment package for the assessments and briefing packages to present along with administering the PRT.

58.9.d. The DCIS Health and Wellness Handbook prepared and updated by the NPM will aid special agents in developing their regular fitness activities. **All OIG DoD criminal investigators will receive a copy of the handbook from their first line supervisor upon hire. The NPM is responsible for distributing all updates to the field.**

58.10. Regular Fitness Maintenance/Improvement Activity

58.10.a. Special agents are encouraged to participate in PT. To this end, 4 hours of official on-duty time per week are authorized, provided that the criminal investigator participates in the PRT and the duty schedule otherwise permits it. Special agents using 4 hours of official on-duty time per week for PT cannot also use physical fitness time under OIG Instruction 6100.2, "Physical Fitness Program."

58.10.b. The 4 hours may be taken in any increment up to the maximum 2 hours at any given time. The 4 hours per week are authorized on a "use it or lose it" weekly basis only and cannot be accumulated. The PT time begins when the criminal investigator leaves his/her office/desk and includes travel time, warmups, shower, and PT activity.

58.10.c. The PT time can be performed during work hours, before work, after work, or on weekends. Law Enforcement Availability Pay hours will not be claimed for PT time taken while in a leave status. ("Leave status" is defined in SAM Chapter 54.)

58.10.d. The PT selected by each criminal investigator should promote maintenance or improvement in one or more of the PRT areas. Examples of approved activities include running, jogging, walking, weight training, aerobics, bicycling while wearing a helmet, swimming, rowing, stair climbing, calisthenics, noncontact martial arts, yoga, and stationary skiing. Supervisors, in conjunction with Health and Wellness Instructors, may approve additional nonhazardous activities. Competitive, contact, and dangerous activities of any kind are not approved as part of this program. Such prohibited activities include soccer, racquetball, handball, basketball, contact martial arts, and football.

58.10.e. To minimize the risk of injury during PT, special agents will not engage in on-duty PT under hazardous conditions (e.g., conditions of poor visibility, weather extremes). Off-duty injuries incurred by special agents under hazardous conditions will not be considered as on-the-job.

58.10.f. PT injuries that occur during or outside of normal duty hours could be considered job-related injuries if it can be established that they occurred as part of an authorized

agency fitness program. Therefore, it is important to maintain accurate and complete activity records on DCIS Form 54.

58.11. Confidentiality—Physical Readiness Test

58.11.a. Fitness information is subject to the provisions of the Privacy Act and HIPAA and will be maintained in a secure manner.

58.11.b. Instructors will have access only to information needed to administer the PRT and assessments. The file should contain PRT results, a copy of the DCIS Health Questionnaire (not medical exam results) and a record of the special agent's health and wellness assessment. These records shall be treated in the strictest confidence and accessed only on a need-to-know basis.

58.11.c. All fitness information maintained by the NPM will be in a locked secure file cabinet to which only he or she has access.

58.11.d. As a matter of policy, the NPM is not authorized to disclose fitness information about an individual to anyone except to the FOH MRO staff, DCIS managers, and Health and Wellness Instructors on a need-to-know basis.

58.11.e. The NPM is responsible for maintaining an agency-wide database tracking the results of the PRT.

LIST OF ATTACHMENTS

<u>Attachment</u>	<u>Title</u>
A	Sample Annual Field Office Program Profile
B	Medical Qualifications Standards OIG DoD GS-1811 Criminal Investigator
C	Sample Initial Waiver Request
D	Sample Medical Standards Waiver Decision
E	Sample Waiver Renewal
F	DCIS Health Screening Questionnaire
G	PRT Assessment Protocols
H	Cooper Institute Age and Gender Norms
I	Health and Wellness Assessment Checklist

ATTACHMENT A

SAMPLE ANNUAL FIELD OFFICE PROGRAM PROFILE

MEMORANDUM FOR DCIS HEALTH AND WELLNESS NATIONAL PROGRAM
MANAGER
THROUGH SPECIAL AGENT IN CHARGE, CENTRAL FIELD OFFICE
ASSISTANT SPECIAL AGENT IN CHARGE, CENTRAL FIELD OFFICE

SUBJECT: Annual Field Office Program Profile

Assessments

Voluntary annual health and wellness assessments have been completed for the following agents:

Quincy Quads Chicago

Gabby Garbo St. Louis

Danger Ranger Chicago

Waivers Granted for PRT

Harry Hamstring (Kansas City) Medical (Spring)

Tammy Tightrope (Wichita) Medical (Spring/Fall)

Jim Lacy (St. Louis) Administratively Unavailable (Spring)

Health and Wellness Instructor Status

<u>Instructor</u>	<u>Training History</u>	<u>First Aid/CPR</u>	<u>Offices Covered</u>
SA Barney Biceps	9/2/99 (FLETC) 10/31/03 (Cooper)	2/5/11	Chicago Indianapolis
SA Lonnie Leggs	3/5/04 (FLETC)	2/5/11	Sioux Falls
SA Karen Cardio	3/15/05 (FLETC)	3/15/11	St. Louis
SA Stretch Henderson	1/25/02 (FLETC)	11/14/11	Kansas City Wichita Minneapolis
SA Willy Wellness	3/14/05 (FLETC)	3/15/11	Dayton

Columbus
Cleveland

Projected Training for Health and Wellness Instructors

Barney Biceps	Cooper	Refresher training
Sue Sharp	FLETC	Basic Instructor training
Bob Bench	Cooper	Advanced training

Comments

SA Barney Biceps' first aid and CPR certification have expired due to being called up to active duty. Upon return SA Biceps will renew his certification.

Program Status and Recommendations

Provide a short summary of the effectiveness/viability of the Program, issues that need to be addressed, and recommendations for improvement.

Karen Cardio
Health and Wellness Coordinator
Central Field Office

ATTACHMENT B

MEDICAL QUALIFICATION STANDARDS **OIG DoD GS-1811 CRIMINAL INVESTIGATOR**

GENERAL

The position requires the employee to be in excellent physical condition and capable of strenuous physical exertion without hazard to himself/herself or others. The position requires irregular unscheduled hours, personal risks, exposure to all kinds of weather, considerable travel, and rigorous exertion under adverse environmental conditions.

HEARING

Hearing loss exceeding a 25-decibel average in either ear in the conversational and speech range (500, 1000, 2000 cycles) is disqualifying. If an applicant or criminal investigator fails to meet these requirements, he/she may proceed to more sophisticated testing as determined by the FOH MRO.

VISION

Corrected vision of no less than 20/20 in one eye and 20/30 in the other eye is required. Near vision correctable at 13 ft. to 16 ft. to 20/20 to 20/30.

FUNCTIONS

- Heavy lifting (more than 45 pounds)
- Heavy carrying (more than 45 pounds)
- Reaching above the shoulder
- Use of fingers
- Use of both hands
- Walking (4-6 hours)
- Standing (4-6 hours)
- Both legs required
- Operation of motor vehicle
- Ability for rapid mental and muscular coordination simultaneously
- Both eyes required
- Depth perception

ENVIRONMENTAL FACTORS

- Outside work
- Unusual fatigue factors
- Working closely with others
- Working alone
- Protracted or irregular work hours

CRITICAL DEMANDS

- Use of firearms
- Appropriate reaction to unexpected emergencies
- Ability to sustain temporary or long-term assignments to overseas locations where medical facilities may be below those normally offered within the United States.

DISEASES/DEFECTS

Tuberculosis – Under no condition may persons with active tuberculosis be employed. Persons with arrested tuberculosis may be employed if medical evidence shows that the condition has been arrested and the criminal investigator is generally in good health. An individual may be approved on the recommendation of the FOH MRO when there is proof that a minimal tuberculosis lesion has been arrested for at least 5 years.

Diabetes – The Office of Personnel Management determining Medical Eligibility for Employment (Supplement 339-21) does not preclude the employment of diabetics in rigorous duty positions provided the condition is controlled. Persons who have never experienced diabetic coma and who have their condition under control may be considered physically qualified to perform the duties of a criminal investigator.

Peptic Ulcer – A history of peptic ulcers is usually not an acceptable condition for rigorous duty positions unless the FOH MRO is able to determine that the ulcer has healed.

Blood Pressure – The following standards may be applied in uncomplicated cases of high blood pressure where all other evidence relating to the circulatory system is favorable. In the case of initial employment, waivers will not be granted. Cases exceeding a maximum systolic 150, diastolic 90 must be referred to the FOH MRO for an opinion.

Diseases – When medical evidence indicates the existence and/or history of one of the following diseases or physical defects, secure the opinion of the FOH MRO: communicable diseases (e.g., syphilis, gonorrhea, Lymphopathia venereum, lymphogranuloma, Acquired Immune Deficiency Syndrome (AIDS), or AIDS-related complex) mental illness, epilepsy, organic heart disease, severe crippling conditions, missing major extremities.

Laboratory Tests – Each criminal investigator will undergo appropriate blood tests and urinalysis to determine if he/she is under the influence of any type of dangerous drug or narcotic, or has any communicable diseases. A criminal investigator found under the influence of a

dangerous drug or narcotic will be disqualified. The only exception will be those special agents who are on prescribed drugs/narcotics. In such cases, the FOH MRO will offer an opinion about the special agent's suitability for employment.

ATTACHMENT C

SAMPLE INITIAL WAIVER REQUEST

MEMORANDUM FOR OIG MEDICAL REVIEW BOARD

THROUGH SPECIAL AGENT IN CHARGE

DCIS HEALTH AND WELLNESS NATIONAL PROGRAM MANAGER

SUBJECT: Waiver Request

I recently received a Medical Review Form dated [date] signed by [name of reviewing physician]. [He/she] states that I do not meet the [Agency standards] qualifying me to perform the essential functions of my job due to [medical condition]. I request that the OIG Medical Review Board review this request and issue a waiver of the (medical condition) standards for an OIG 1811 Criminal Investigator.

My condition is the result of [.....]. Since returning to work fulltime on (date), I have successfully performed all duties and training required by my position. I have successfully completed the DCIS physical readiness test, handgun qualification, and shotgun familiarization requirements. My abilities to perform the required duties of a DCIS criminal investigator have not been hindered or limited as a result of my condition. I currently engage in a physical readiness routine 3 days a week that encompasses weight training and cardiovascular events. I have had no physical or medical setbacks since returning to work. I continue to be active in my job and personal activities. I have participated and accomplished the requirements of this job and will continue to do so. It is for these reasons that I request a waiver from the OIG's (xxxxx) standards.

I agree to notify my immediate supervisor and the DCIS Health and Wellness National Program Manager if I change job positions or if my medical condition further deteriorates.

Investigator [Signature]

[Date]

Supervisor verification:

I concur with the above statements of [name] that s/he can perform his/her job safely and efficiently within the dictates of the medical waiver.

Supervisor [Signature]

[Date]

ATTACHMENT D

SAMPLE MEDICAL STANDARDS WAIVER DECISION

(DATE)

MEMORANDUM FOR [AGENT'S NAME]

SUBJECT: Medical Standards Waiver Decision

On [date], [name of reviewing physician] signed the Medical Review Form notifying you that the final results of your medical testing had been reviewed and it was found that you had [a condition that did not meet the agency standard]. This document indicated that you did not meet the medical standard for [whatever the issue is], related to performing your duties [with the Defense Criminal Investigation Service]. You appealed this decision and requested that the Deputy Assistant Inspector General for Investigations, Internal Operations Directorate, review information relative to your ability to meet the GS-1811 criminal investigator medical qualifications standards, despite this medical condition.

In order to render a decision, the OIG Medical Review Board considered: written documentation; the specific job requirements of your position; the GS-1811 criminal investigator medical qualification standards; the final results of the medical review; your performance capabilities in that position; documentation submitted by you, your supervisor, and others on your behalf; and our knowledge of those duties.

The Board has determined that the documentation supports a finding that you are able to perform the full range of essential duties specific to your position, without undue risk to yourself or others. Therefore, it is the Board's decision that you be granted a waiver regarding [the specific condition for which the waiver is being given] described in your Medical Review Form.

Since medical conditions may improve, deteriorate, or resolve, if your medical condition should change, you must notify your immediate supervisor and the NPM for guidance. If your medical condition does deteriorate, you may apply for a renewal of this waiver by submitting the attached medical waiver renewal form. Your request for a renewal should only come after completing your next scheduled medical review and you are in receipt of its results.

I want to extend best wishes for continued success in future positions and thank you for your compliance with the Medical Standards Program.

[Name]

ATTACHMENT E
SAMPLE WAIVER RENEWAL

[Date]

MEMORANDUM FOR OIG MEDICAL REVIEW BOARD

THROUGH SPECIAL AGENT IN CHARGE
DCIS HEALTH AND WELLNESS NATIONAL PROGRAM MANAGER

SUBJECT: Waiver Renewal

I recently received a Medical Review Form dated [date] signed by [name of reviewing physician]. [He/she] states that I do not meet the [Agency standards] qualifying me to perform the essential functions of my job due to [medical condition]. This issue was raised on my initial medical review that was signed on [date] while employed with [DCIS]. I appealed the medical standards and was issued a waiver enabling me to continue my duties as a criminal investigator on [date].

Since the initial review, my condition has deteriorated. I have continued to perform the full range of my duties as a criminal investigator without undue risk to others or myself. I am requesting a renewal of my waiver for [medical condition].

I agree to notify my immediate supervisor and the DCIS Health and Wellness National Program Manager if I change job positions or if my medical condition further deteriorates.

I have attached a copy of the waiver issued by the OIG MEDICAL REVIEW BOARD and the Medical Review Form issued by [name of reviewing physician].

Investigator [Signature]

[Date]

Supervisor verification:

I concur with the above statements of [name], that s/he can perform his/her job safely and efficiently within the dictates of the medical waiver.

Supervisor [Signature]

[Date]

ATTACHMENT F

HEALTH SCREENING QUESTIONNAIRE

Name: _____

The purpose is to identify individuals who may be at risk in taking the DCIS Physical Readiness Test (PRT) and recommend a medical examination prior to taking the PRT.

Employees are required to answer the following questions. The questions were designed, in consultation with occupational health physicians, to identify individuals who may be at risk when taking the DCIS PRT. The Health Screening Questionnaire (HSQ) is not a medical examination. Any medical concerns you have that place you or your health at risk should be reviewed with the Federal Occupational Health (FOH) Medical Review Officer and/or your personal physician prior to participating in the PRT.

Agents who respond with a ‘Yes’ answer to any of the following question will be prohibited from taking the PRT until such issue(s) are addressed and cleared by the FOH Medical Review Officer.

Check ‘Yes’ or ‘No’ in response to the following questions:

1) Since your last FOH physical have you at any time (during physical activity or while resting) experienced pain, discomfort, or pressure in your chest?

☐ **Y**

☐ **N**

2) Since your last FOH physical have you experienced difficulty breathing or shortness of breath, dizziness, fainting, or blackout?

☐ **Y**

☐ **N**

3) Since your last FOH physical are you aware or have you been told that you have a blood pressure with systolic (top #) greater than 140 or diastolic (bottom #) greater than 90 or an abnormal blood pressure?

☐ **Y**

☐ **N**

4) Since your last FOH physical have you ever been diagnosed or treated for any heart disease, heart murmur, chest pain (angina), palpitations (irregular beat), or heart attack?

☐ Y

☐ N

5) Since your last FOH physical have you had heart surgery, angioplasty, or a pacemaker, valve replacement, or heart transplant?

☐ Y

☐ N

6) Since your last FOH physical are you aware or have you been told you have a resting pulse greater than 100 beats per minute?

☐ Y

☐ N

7) Do you have any muscular, skeletal, or joint condition that could be aggravated or made worse by the PRT?

☐ Y

☐ N

8) Since your last FOH physical do you have personal experience or doctor's advice of any other medical or physical reason that would prohibit you from taking the PRT?

☐ Y

☐ N

9) Since your last FOH physical has your personal physician or the DCIS Medical Review Officer recommended against taking the PRT because of asthma, diabetes, epilepsy, elevated cholesterol, or a hernia?

☐ Y

☐ N

10) During your last FOH Medical Exam were you cleared to participate in the PRT?

☐ Y

☐ N

ATTACHMENT G

PRT ASSESSMENT PROTOCOLS

After safety, the most important element in the administration of the PRT is following the proper protocol. If possible, the sequence of testing and the equipment used during testing should be the same. The purpose of this is to diminish, if not avoid, the possibility of testing inconsistencies. The order for testing push-ups, sit-ups, and flexibility is left to the discretion of the Health and Wellness Instructor. It is recommended that the cardiovascular assessment (1.5-mile run or 3-mile walk) be the final event. The reasoning behind this is that the cardiovascular assessment taxes virtually all major muscle groups, which may have an adverse impact on the other events if they are performed after this test. If there are multiple instructors, it may be advisable to divide the participants up into even sections and rotate them among the push-up, sit-up, and flexibility tests.

Prior to the participants beginning, demonstrate the PRT event, except for the cardiovascular assessment, to ensure that the special agents fully understand the proper protocol and disqualifiers for each event. After the demonstration of each event, the instructors should ask if there is anyone who is unable to perform the event due to injury or illness, and should ensure that special agents with limited medical clearances do not participate if the particular test is restricted.

In order for the PRT to be meaningful, the testing protocols and disqualifiers **must** be followed for each of the five tested components of the assessment. The assessment charts for the individual events are located at the end of this section.

Prior to performing the assessments, warmup activities should be performed. These activities should include light calisthenics, stretching, and other low-intensity activities. The purpose of the warmup is to provide a mild stimulus to the muscle groups that will be used during the remainder of the assessment, thereby reducing the risk of injury.

FLEXIBILITY (TRUNK FLEXION) TEST

The flexibility testing protocol should be explained and demonstrated to all participants prior to performing the test. Following the demonstration, the instructors should ask if there are any questions and ascertain if there is anyone who feels he or she cannot perform the assessment. As previously mentioned, the instructors must also ensure that special agents with limited medical clearances do not perform restricted exercises.

1. Recommend to the participants that it is to their advantage to remove their shoes prior to performing this assessment. Depending on the style or type of shoe being worn, scores could be diminished due to the thickness of the sole. Additionally, removing the shoes creates a distance more similar to that of touching the floor while standing. If a participant does not wish to remove his or her shoes, he or she is not required to do so.
2. The participant will be seated on the floor with feet flush against the flexibility box. The feet should be 8 inches apart with toes pointing up.

3. The participant's legs must be straight and the calves **must** remain in contact with the floor at all times. If it is difficult for the criminal investigator to do this, other participants may hold the special agent's legs down by placing one hand above the knee and the other hand below the knee on the shin. Never allow assisting participants to hold the special agent's legs down by pressing on the knees due to the potential for injury. It is important that the assisting participants do not otherwise interfere or assist with the special agent's assessment.
4. When the criminal investigator is ready to perform the assessment, advise him or her to take a deep breath and exhale slowly while pushing the slide forward. The fingertips of both hands **must** remain in contact with the slide at all times. Once the criminal investigator has reached his or her farthest extension point, the position **should** be held for a "two count." This will ensure the push was a true measure of the special agent's flexibility rather than a lunge.
5. The participant may have two more attempts, if desired, and the best of the three will be recorded. The criminal investigator is not required to make more than one attempt if he or she does not wish to do so. Measure scores in quarter-inch increments rounding up to the nearest quarter-inch. For example, record a push of 16 1/8 inches as 16 1/4 inches.

Flexibility Disqualifiers

1. The push must be smooth and static. If the participant lunges or pushes the slide in a ballistic manner, the attempt will not count.
2. The fingertips of **both** hands **must** remain in contact with the slide at all times. If one hand comes off the slide during the push, the attempt will not count.
3. The legs must be straight and the calves **must** remain in contact with the ground at all times. If a participant's legs (calves) leave the ground, the attempt will not count. Be sure to advise participants that they may have other special agents assist in holding their legs down.

Sit-Up (Trunk Strength) Test

The sit-up test measures the individual's upper abdominal strength, lower back strength, and muscular endurance. The goal of the test is to perform the maximum number of correct sit-ups in 60 seconds. The testing protocol should be explained and demonstrated to all participants prior to performing the test. Following the demonstration, the instructors should ask if there are any questions and ascertain if there is anyone who feels he or she cannot perform the assessment. As previously mentioned, the instructors must also ensure that special agents with limited medical clearances do not perform restricted exercises.

1. Special agents begin the test lying on their backs with knees bent, heels flat on the floor. A partner may hold the participant's feet down during the test. The participant's hands must be placed on the sides of the head. **Do not** allow the special agents to interlace their

fingers behind the head. As participants become fatigued, there is a tendency to pull with hands, resulting in a risk of hyperextension of the neck.

2. The trunk is raised up and the special agent's elbows **must** touch his or her knees to receive credit for a proper repetition.
3. When returning to the down position, the special agent's shoulder blades **must** touch the floor before beginning the next repetition.
4. Either an instructor or an assisting participant should count the number of properly performed sit-ups. At the conclusion of the test, the assisting participant will give the score to the instructor for recording.
5. If necessary, a participant may rest in the "up" position, but cannot hold on to their legs in order to stay up.
6. Breathing should be as normal as possible; make sure the subject does not hold their breath as in the Valsalva maneuver.

Sit-Up Test Disqualifiers

1. During the "up" phase, if the special agent's elbows do not touch the knees, the sit-up will not be counted.
2. During the "down" phase, if the special agent's shoulder blades do not touch the floor before beginning the next repetition, the sit-up will not be counted.
3. If during the assessment the criminal investigator stops in the "down" position, terminate the test for that individual and record the number of correctly executed sit-ups to that point.

Push-Up Test

Push-ups are used to assess the strength and endurance of the upper body muscle groups. The goal of the test is to perform the maximum number of correct push-ups in 60 seconds. The testing protocol should be explained and demonstrated to all participants prior to performing the test. Following the demonstration, the instructors should ask if there are any questions and ascertain if there is anyone who feels he or she cannot perform the assessment. As previously mentioned, the instructors must also ensure that special agents with limited medical clearances do not perform restricted exercises.

1. Special agents begin the test in the "up" position with their elbows locked out, body straight, hands placed slightly wider than shoulder-width apart, with fingers pointing

forward and both feet on the floor. A partner should be positioned either in front or to the side of the participant to observe, along with the instructor(s), the proper execution of the push-ups.

2. The participant must lower his or her body, while keeping the back straight, until the shoulders drop **below** the level of the elbows.
3. The participant must return to the “up” position, pushing until full elbow extension is achieved (without locking out the elbows) to receive credit for a properly executed push-up.
4. The assisting partner should count the number of properly executed push-ups and give this number to the instructor at the conclusion of the test.
5. If necessary, participants may rest in the “up” position.
6. The total number of correct push-ups in 1 minute is recorded as the score.

******Since traditional push-up standards are not available, females aged 50 or older may elect to perform modified push-ups. The modified push-up is performed on the hands and knees with the back straight and the hands slightly in front of the shoulders in the up position.

Push-Up Test Disqualifiers

1. During the “up” phase, if the special agent’s elbows do not fully extend before beginning the next repetition, do not count the push-up.
2. During the “down” phase, if the special agent’s shoulders are not lowered past the elbow level before returning to the “up” position, do not count the push-up.
3. If during the assessment, the criminal investigator stops in the “down” position, including going to one’s knees (except for modified position), terminate the test for that individual and record the number of correctly executed push-ups to that point.

CARDIOVASCULAR ASSESSMENTS

The 1.5-mile run and 3-mile walk are used to assess an individual’s cardiovascular endurance and fitness. A criminal investigator may choose to walk the entire 1.5 miles, but his or her performance will be evaluated using the 1.5-mile run assessment chart. The protocols for each of the above-mentioned exercises will be detailed separately. The testing protocols should be explained to all participants prior to performing the assessment. Following the explanation, the instructors should ask if there are any questions and ascertain if there is anyone who feels he or she cannot perform the assessment. As previously mentioned, the instructors must also ensure that special agents with limited medical clearances do not perform restricted exercises.

1.5-Mile Run

1. If possible, the instructors should have more than one stopwatch available and have an assistant to count laps if there is a large group of participants being tested.
2. Instructors should caution participants about overexerting themselves and advise them to listen to their bodies and pace themselves. Non-runners may want to follow the guidance of “running the straights and walking the curves.”
3. If running on a quarter-mile track, the participants must complete six laps. The quickest route is on the inside lane, however, track courtesy should be observed. If a slower runner is about to be overcome by a faster runner, the faster runner should yell, “track!” Upon hearing this, the slower runner should move to the right to allow the faster runner to pass and then return to the inside lane once it is safe to do so.
4. All participants should start at the same time, preferably with the faster runners in the front. The instructors start the stopwatches on the word “GO!” Remember, it is advisable to have more than one timekeeper in the event of a stopwatch malfunction.
5. As participants pass by the timekeeper, the times should be called out. If running on a quarter-mile track, inform participants when they are at the halfway, mile, and final lap points.
6. As participants finish, call out their final times but ask them to remember it as well. When the assessment is completed, the special agents should check with the recorder to verify their time. All participants must complete the entire assessment unless they become ill or injured. **NO** pro-rating of times is allowed for slower participants.
7. As participants finish the assessment they **must** walk one lap (or the equivalent of a quarter mile if not on a track) as a cool down. This cool down should be performed on the outside lanes of the track or testing area in order to leave the inside lanes open for participants who are still running. At least one instructor **must** remain at the track until all participants have completed their cool down lap.
8. If a participant gets sick or injured during the test, instruct him or her to move quickly and safely to the outside of the track (or other designated area) so the instructors will know there is a problem.
9. During this type of testing, it is critical to have some type of medical support in place, especially during the 1.5-mile run. Emergency procedures should be formulated, approved by management, distributed and posted, and rehearsed.
10. Dangerous climate conditions (such as hot/humid weather) should be avoided and water or other fluids should be made available to the special agents upon completion of the assessment. Instructors should assess the participants’ condition upon completion of the test to ensure that everyone is all right.

3-Mile Walk

The protocol for the 3-mile walk is the same as that of the 1.5-mile run except that the distance to be completed is 3 miles. In addition, advise participants doing the 3-mile walk of the following.

1. In order for the measurement charts for the 3-mile walk to be accurate, participants **must** keep one foot on the ground for the duration of the assessment. If an individual begins to “jog or run” the course, the participant will be disqualified because the measurement will be skewed.
2. If runners and walkers are to be assessed at the same time on the same track, it is advisable to have the walkers perform the assessment to the right of the innermost lane until the runners are finished. This will minimize the risk of collision and injury due to special agents constantly shifting lanes. Once the runners are finished, the walkers should proceed to the innermost lane.

OPTIONAL BODY COMPOSITION TEST

Body composition is an important health-related component of physical readiness. Therefore, it is included as an option as part of the special agent’s annual health and wellness assessment.

1. In order to establish consistency, measure **every** criminal investigator on the **right** side of the body. The body composition standards are based on measurements taken only on the right side; therefore, this is the recommended procedure.

Exceptions. Common sense should dictate exceptions. For example, if a participant has significant scar tissue in a tested area on the right side of the body that will prevent an accurate readout, then use the left side of the body.

2. It is recommended that metal, spring-loaded, skinfold calipers be used rather than plastic ones. Although both types of calipers lose some accuracy after excessive use, the spring-loaded calipers may be re-calibrated whereas the plastic ones cannot.
3. It is important that persons who are waiting to be tested stand at least 20 feet away. This provides an essential degree of privacy and confidentiality to the individual who is being measured. Whenever possible, match the gender of the testing instructor with the participant. All readings should be recorded discreetly.
4. Proper technique is critical in obtaining accurate skinfold readings. Detailed below are the basic guidelines identifying the proper procedures for performing skinfold assessments. Following these guidelines will reduce measurement errors and increase consistency and accuracy.
 - If possible, the instructor measuring the skinfolds should not be the one recording them. Another instructor should record the values as the measuring instructor

reads them from the calipers. It is helpful if the assisting instructor quietly repeats the values to ensure they are properly recorded.

- Practice as much as possible. One of the greatest sources of error (inaccurate or inconsistent readings) is variance between instructors due to an inability to accurately locate and measure the skinfold.
5. Take all measurements from the right side of the body, if possible.
- Make sure the skinfold site is dry and free of lotions. Wet skin may be easier to grasp and this additional skin would improperly increase the skinfold reading. Skinfolts with lotion on them are more difficult to grasp and may affect the accuracy of the measurement.
 - Ensure that only the fold of the skin—with its subcutaneous fat—is being measured at the appropriate site. If there is difficulty in distinguishing fat from muscle, ask the individual to contract and relax the underlying muscle. This will help identify the proper skinfold to be measured.
 - Use an upside-down “U grip” with the thumb and index finger to grasp the skinfold.
 - Place the calipers right below the thumb and index finger and at a depth that is equal to the skinfold. The calipers, as well as the thumb and index finger, should be perpendicular to the fold of the skin.
 - Once the tension has been completely released from the calipers, the skinfold measurement should be taken within 2-3 seconds. This allows the tips of the calipers to compress the fat cells and stabilize at a particular value. Measurements are made in millimeters and can be recorded to the nearest 0.5mm (Lange Calipers) or 0.1mm if other calipers are used.
 - A minimum of two skinfold measurements should be taken at each site. The pinch should be released after each measurement to avoid compressing the fat cells with your fingers. If the first two readings are the same, that value may be recorded. If the readings vary by more than 1 millimeter, take up to three more readings to obtain a consistent value. If a consistent measurement cannot be obtained after five attempts, stop measuring at that site. After repeated measurements, the skinfold can become compressed, preventing an accurate reading from being obtained. Continue measuring the other sites and then return to the previous site. If a consistent value still cannot be achieved after five more attempts, use the average of the five readings for that site.

Male Skinfold Sites

1. **Chest:** In a standing position, have the subject place both arms at his sides, relaxing the pectoral (chest) muscle. Visualize an imaginary line running diagonally from the front crease of the armpit to the nipple and locate the midpoint between these two landmarks. Using an upside-down “U grip,” take a diagonal skinfold at the midpoint, making sure to separate the fat tissue from the muscle tissue. If you have difficulty in distinguishing fat from muscle, have the individual place his right hand on your shoulder and press down. This will cause the pectoral muscle to contract and assist in taking the correct measurement.
2. **Abdomen:** Have the subject stand straight and relaxed. Locate the site approximately 1 inch to the right of the navel. Using an upside-down “U-grip,” take a vertical skinfold at the site.
3. **Thigh:** While standing, have the subject place his right heel on the inside of his left foot. This should flex the right knee slightly and relax the thigh muscles. The measurement site is located approximately midway between the hip joint and the top of the kneecap. Using an upside-down “U-grip,” take a vertical skinfold measurement at the site.

Female Skinfold Sites

1. **Triceps:** Have the subject stand with arms relaxed at the sides and the right elbow bent at a 90-degree angle. The measurement site is located on the back of the upper arm approximately halfway between the top bony projection of the shoulder and the bony protuberance of the elbow. Using an upside-down “U-grip,” take a vertical skinfold measurement at the site.
2. **Suprailiac:** With the subject standing straight, have **her** raise her shirt and lower the top of her shorts slightly to expose the suprailiac site. Have her locate the top ridge of the hipbone at about waist level and then visualize an imaginary line from the front of the armpit intersecting this site. The measurement area is located where this line intersects with the hipbone. Using an upside-down “U-grip,” take a diagonal skinfold measurement at the site.
3. **Thigh:** The thigh skinfold site for the female is identical to that of the male. Thus, the same protocol as described above will be followed.

ATTACHMENT H

COOPER INSTITUTE

AGE AND GENDER NORMS*

3-Mile Walking Test (No Running)

Time (Minutes)

<i>Fitness Category</i>		<i>20-29</i>	<i>30-39</i>	<i>40-49</i>	<i>50-59</i>
I. Very Poor	(men)	> 46:00*	>49:00	>52:00	>55:00
	(women)	>48:00	>51:00	>54:00	>57:00
II. Poor	(men)	42:01-46:00	44:31-49:00	47:01-52:00	50:01-55:00
	(women)	44:01-48:00	46:31-51:00	49:01-54:00	52:01-57:00
III. Fair	(men)	38:31-42:00	40:01-44:30	42:01-47:00	45:01-50:00
	(women)	40:31-44:00	42:01-46:30	44:01-49:00	47:01-52:00
IV. Good	(men)	34:00-38:30	35:00-40:00	36:30-42:00	39:00-45:00
	(women)	36:30-40:30	37:30-42:00	39:00-44:00	42:00-47:00
V. Excellent	(men)	<34:00	<35:00	<36:30	<39:00
	(women)	<36:00	<37:30	<39:00	<42:00

* < means “less than,” > means “more than”

The walking test covering 3 miles in the fastest time possible *without* running can be done on a track or over any accurately measured distance. As with running, take the test after you have been training for at least 6 weeks, when you feel rested. Dress to be comfortable.

* Reprinted with permission of The Cooper Institute, “Physical Fitness Assessment and Norms,” Dallas, TX

CARDIORESPIRATORY FITNESS TESTS

Males

	Age 20-29				Age 30-39				
	Balke Treadmill (time)	Max $\dot{V}O_2$ (ml/kg/min.)	12 min. Run Distance (miles)	1.5 Mile Run (time)	Balke Treadmill (time)	Max $\dot{V}O_2$ (ml/kg/min.)	12 min. Run Distance (miles)	1.5 Mile Run (time)	
%									
99	32:00	61.2	2.02	8:22	30:00	58.3	1.94	8:49	
95	28:31	56.2	1.88	9:10	27:11	54.3	1.82	9:31	S
90	27:00	54.0	1.81	9:34	26:00	52.5	1.77	9:52	
85	26:00	52.5	1.77	9:52	24:45	50.7	1.72	10:14	
80	25:00	51.1	1.73	10:08	23:30	48.9	1.67	10:38	E
75	23:40	49.2	1.68	10:34	22:30	47.5	1.63	10:59	
70	23:00	48.2	1.65	10:49	22:00	46.8	1.61	11:09	
65	22:00	46.8	1.61	11:09	21:00	45.3	1.57	11:34	
60	21:15	45.7	1.58	11:27	20:20	44.4	1.55	11:49	G
55	21:00	45.3	1.57	11:34	20:00	43.9	1.53	11:58	
50	20:00	43.9	1.53	11:58	19:00	42.4	1.49	12:25	
45	19:26	43.1	1.51	12:11	18:15	41.4	1.46	12:44	
40	18:50	42.2	1.49	12:29	18:00	41.0	1.45	12:53	F
35	18:00	41.0	1.45	12:53	17:00	39.5	1.41	13:25	
30	17:30	40.3	1.43	13:08	16:15	38.5	1.38	13:48	
25	17:00	39.5	1.41	13:25	15:40	37.6	1.36	14:10	
20	16:00	38.1	1.37	13:58	15:00	36.7	1.33	14:33	P
15	15:00	36.7	1.33	14:33	14:00	35.2	1.29	15:14	
10	14:00	35.2	1.29	15:14	13:00	33.8	1.25	15:56	
5	12:00	32.3	1.21	16:46	11:10	31.1	1.18	17:30	
1	8:00	26.6	1.05	20:55	8:00	26.6	1.05	20:55	VP

n = 2,606

n = 13,158

Total n = 15,764

Balke treadmill, max $\dot{V}O_2$, and 12 min. run are included for informational purposes only and are **NOT** part of the DCIS PRT protocol.

CARDIORESPIRATORY FITNESS TESTS

Males

% Age	Age 40-49				Age 50-59				
	Balke Treadmill (time)	Max $\dot{V}O_2$ (ml/kg/min.)	12 min. Run Distance (miles)	1.5 Mile Run (time)	Balke Treadmill (time)	Max $\dot{V}O_2$ (ml/kg/min.)	12 min. Run Distance (miles)	1.5 Mile Run (time)	
99	29:06	57.0	1.90	9:02	27:15	54.3	1.82	9:31	
95	26:16	52.9	1.79	9:47	24:00	49.7	1.69	10:27	S
90	25:00	51.1	1.73	10:09	22:00	46.8	1.61	11:09	
85	23:14	48.5	1.66	10:44	20:31	44.6	1.55	11:45	
80	22:00	46.8	1.61	11:09	19:35	43.3	1.52	12:08	E
75	21:02	45.4	1.58	11:32	18:32	41.8	1.47	12:37	
70	20:15	44.2	1.54	11:52	18:00	41.0	1.45	12:53	
65	20:00	43.9	1.53	11:58	17:00	39.5	1.41	13:25	
60	19:00	42.4	1.49	12:25	16:10	38.3	1.38	13:53	G
55	18:02	41.0	1.45	12:53	16:00	38.1	1.37	13:58	
50	17:34	40.4	1.44	13:05	15:02	36.7	1.33	14:33	
45	17:00	39.5	1.41	13:25	14:56	36.6	1.33	14:35	
40	16:12	38.4	1.38	13:50	14:00	35.2	1.29	15:14	F
35	15:38	37.6	1.36	14:10	13:05	33.9	1.26	15:53	
30	15:00	36.7	1.33	14:33	12:38	33.2	1.24	16:16	
25	14:20	35.7	1.31	15:00	12:00	32.3	1.21	16:46	
20	13:35	34.6	1.28	15:32	11:10	31.1	1.18	17:30	P
15	12:45	33.4	1.24	16:09	10:15	29.8	1.14	18:22	
10	11:40	31.8	1.20	17:04	9:15	28.4	1.10	19:24	
5	10:00	29.4	1.13	18:39	7:30	25.8	1.03	21:40	
1	7:00	25.1	1.01	22:22	4:20	21.3	0.90	27:08	VP

n = 16,534

n = 9,102

Total n = 25,636

Balke treadmill, max $\dot{V}O_2$, and 12 min. run are included for informational purposes only and are **NOT** part of the DCIS PRT protocol.

CARDIORESPIRATORY FITNESS TESTS

Males

	Age 60-69				Age 70-79				
	Balke Treadmill (time)	Max $\dot{V}O_2$ (ml/kg/min.)	12 min. Run Distance (miles)	1.5 Mile Run (time)	Balke Treadmill (time)	Max $\dot{V}O_2$ (ml/kg/min.)	12 min. Run Distance (miles)	1.5 Mile Run (time)	
%									
99	25:02	51.1	1.74	10:09	24:00	49.7	1.69	10:27	
95	21:33	46.1	1.60	11:20	19:00	42.4	1.49	12:25	S
90	19:30	43.2	1.51	12:10	17:00	39.5	1.41	13:25	
85	18:00	41.0	1.45	12:53	16:00	38.1	1.37	13:57	
80	17:00	39.5	1.41	13:25	14:34	36.0	1.32	14:52	E
75	16:00	38.1	1.37	13:58	13:25	34.4	1.27	15:38	
70	15:00	36.7	1.33	14:33	12:27	33.0	1.23	16:22	
65	14:30	35.9	1.31	14:55	12:00	32.3	1.21	16:46	
60	13:51	35.0	1.29	15:20	11:00	30.9	1.17	17:37	G
55	13:04	33.9	1.26	15:53	10:30	30.2	1.15	18:05	
50	12:30	33.1	1.23	16:19	10:00	29.4	1.13	18:39	
45	12:00	32.3	1.21	16:46	9:20	28.5	1.11	19:19	
40	11:21	31.4	1.19	17:19	9:00	28.0	1.09	19:43	F
35	10:49	30.6	1.17	17:49	8:21	27.1	1.07	20:28	
30	10:00	29.4	1.13	18:39	7:38	26.0	1.04	21:28	
25	9:29	28.7	1.11	19:10	7:00	25.1	1.01	22:22	
20	8:37	27.4	1.08	20:13	6:00	23.7	0.97	23:55	P
15	7:33	25.9	1.03	21:34	5:00	22.2	0.93	25:49	
10	6:20	24.1	0.99	23:27	4:00	20.8	0.89	27:55	
5	4:55	22.1	0.93	25:58	3:00	19.3	0.85	30:34	
1	2:29	18.6	0.83	31:59	2:00	17.9	0.81	33:30	VP

n = 2,682

n = 467

Total n = 3,149

Balke treadmill, max $\dot{V}O_2$, and 12 min. run are included for informational purposes only and are **NOT** part of the DCIS PRT protocol.

CARDIORESPIRATORY FITNESS TESTS

Females

	Age 20-29				Age 30-39				
	Balke Treadmill (time)	Max $\dot{V}O_2$ (ml/kg/min.)	12 min. Run Distance (miles)	1.5 Mile Run (time)	Balke Treadmill (time)	Max $\dot{V}O_2$ (ml/kg/min.)	12 min. Run Distance (miles)	1.5 Mile Run (time)	
%									
99	27:43	55.0	1.84	9:23	26:00	52.5	1.77	9:52	
95	24:24	50.2	1.71	10:20	22:06	46.9	1.62	11:08	S
90	22:30	47.5	1.63	10:59	20:34	44.7	1.56	11:43	
85	21:00	45.3	1.57	11:34	19:03	42.5	1.50	12:23	
80	20:04	44.0	1.54	11:56	18:00	41.0	1.45	12:53	E
75	19:42	43.4	1.52	12:07	17:30	40.3	1.43	13:08	
70	18:06	41.1	1.46	12:51	16:30	38.8	1.39	13:41	
65	17:45	40.6	1.44	13:01	16:00	38.1	1.37	13:58	
60	17:00	39.5	1.41	13:25	15:02	36.7	1.33	14:33	G
55	16:00	38.1	1.37	13:58	15:00	36.7	1.33	14:33	
50	15:30	37.4	1.35	14:15	14:00	35.2	1.29	15:14	
45	15:00	36.7	1.33	14:33	13:30	34.5	1.27	15:35	
40	14:11	35.5	1.30	15:05	13:00	33.8	1.25	15:56	F
35	13:36	34.6	1.27	15:32	12:03	32.4	1.21	16:43	
30	13:00	33.8	1.25	15:56	12:00	32.3	1.21	16:46	
25	12:04	32.4	1.22	16:43	11:00	30.9	1.17	17:38	
20	11:30	31.6	1.19	17:11	10:20	29.9	1.15	18:18	P
15	10:42	30.5	1.16	17:53	9:39	28.9	1.12	19:01	
10	10:00	29.4	1.13	18:39	8:36	27.4	1.08	20:13	
5	7:54	26.4	1.05	21:05	7:16	25.5	1.02	21:57	
1	5:14	22.6	0.94	25:17	5:20	22.7	0.94	25:10	VP

n = 1,350

n = 4,394

Total n = 5,744

Balke treadmill, max $\dot{V}O_2$, and 12 min. run are included for informational purposes only and are **NOT** part of the DCIS PRT protocol.

CARDIORESPIRATORY FITNESS TESTS

Females

	Age 40-49				Age 50-59				
	Balke Treadmill (time)	Max $\dot{V}O_2$ (ml/kg/min.)	12 min. Run Distance (miles)	1.5 Mile Run (time)	Balke Treadmill (time)	Max $\dot{V}O_2$ (ml/kg/min.)	12 min. Run Distance (miles)	1.5 Mile Run (time)	
%									
99	25:00	51.1	1.74	10:09	21:00	45.3	1.57	11:34	S
95	20:56	45.2	1.57	11:35	17:16	39.9	1.42	13:16	
90	19:00	42.4	1.49	12:25	16:00	38.1	1.37	13:58	
85	17:20	40.0	1.43	13:14	15:00	36.7	1.33	14:33	E
80	16:34	38.9	1.40	13:38	14:00	35.2	1.29	15:14	
75	16:00	38.1	1.37	13:58	13:15	34.1	1.26	15:47	
70	15:00	36.7	1.33	14:33	12:23	32.9	1.23	16:26	G
65	14:14	35.6	1.30	15:03	12:00	32.3	1.21	16:46	
60	13:56	35.1	1.29	15:17	11:23	31.4	1.19	17:19	
55	13:02	33.8	1.25	15:56	11:00	30.9	1.17	17:38	F
50	12:39	33.3	1.24	16:13	10:30	30.2	1.15	18:05	
45	12:00	32.3	1.21	16:46	10:00	29.4	1.13	18:39	
40	11:30	31.6	1.19	17:11	9:30	28.7	1.11	19:10	P
35	11:00	30.9	1.17	17:38	9:00	28.0	1.09	19:43	
30	10:10	29.7	1.14	18:26	8:30	27.3	1.07	20:17	
25	10:00	29.4	1.13	18:39	8:00	26.6	1.05	20:55	VP
20	9:00	28.0	1.09	19:43	7:15	25.5	1.02	21:57	
15	8:07	26.7	1.06	20:49	6:40	24.6	1.00	22:53	
10	7:21	25.6	1.03	21:52	6:00	23.7	0.97	23:55	
5	6:17	24.1	0.98	23:27	4:48	21.9	0.92	26:15	
1	4:00	20.8	0.89	27:55	3:00	19.3	0.85	30:34	

n = 4,834

n = 3,103

Total n = 7,937

Balke treadmill, max $\dot{V}O_2$, and 12 min. run are included for informational purposes only and are **NOT** part of the DCIS PRT protocol.

CARDIORESPIRATORY FITNESS TESTS

Females

	Age 60-69				Age 70-79				
	Balke Treadmill (time)	Max $\dot{V}O_2$ (ml/kg/min.)	12 min. Run Distance (miles)	1.5 Mile Run (time)	Balke Treadmill (time)	Max $\dot{V}O_2$ (ml/kg/min.)	12 min. Run Distance (miles)	1.5 Mile Run (time)	
%									
99	19:00	42.4	1.49	12:25	19:00	42.4	1.49	12:25	
95	15:09	36.9	1.34	14:28	15:00	36.7	1.33	14:33	S
90	13:33	34.6	1.27	15:32	12:50	33.5	1.25	16:06	
85	12:28	33.0	1.23	16:22	11:46	32.0	1.20	16:57	
80	12:00	32.3	1.21	16:46	10:30	30.2	1.15	18:05	E
75	11:04	31.0	1.18	17:34	10:00	29.4	1.13	18:39	
70	10:30	30.2	1.15	18:05	9:15	28.4	1.10	19:24	
65	10:00	29.4	1.13	18:39	8:43	27.6	1.08	20:02	
60	9:44	29.1	1.12	18:52	8:00	26.6	1.05	20:54	G
55	9:11	28.3	1.10	19:29	7:37	26.0	1.04	21:45	
50	8:40	27.5	1.08	20:08	7:00	25.1	1.01	22:22	
45	8:15	26.9	1.06	20:38	6:39	24.6	1.00	22:54	
40	8:00	26.6	1.05	20:55	6:05	23.8	0.98	23:47	F
35	7:14	25.4	1.02	22:03	5:28	22.9	0.95	24:54	
30	6:52	24.9	1.01	22:34	5:00	22.2	0.93	25:49	
25	6:21	24.2	0.99	23:20	4:45	21.9	0.92	26:15	
20	6:00	23.7	0.97	23:55	4:16	21.2	0.90	27:17	P
15	5:25	22.8	0.95	25:02	4:00	20.8	0.89	27:55	
10	4:40	21.7	0.92	26:32	3:00	19.3	0.85	30:34	
5	3:30	20.1	0.87	29:06	2:00	17.9	0.81	33:32	
1	2:10	18.1	0.82	33:05	1:00	16.4	0.77	37:26	VP

n = 1,088

n = 209

Total n = 1,297

Balke treadmill, max $\dot{V}O_2$, and 12 min. run are included for informational purposes only and are **NOT** part of the DCIS PRT protocol.

FLEXIBILITY
Sit and Reach

Males

AGE

%	<20	20-29	30-39	40-49	50-59	60+	
99	> 23.4	>23.0	>22.0	>21.3	>20.5	>20.0	
95	23.4	23.0	22.0	21.3	20.5	20.0	S
90	22.6	21.8	21.0	20.0	19.0	19.0	
85	22.4	21.0	20.0	19.3	18.3	18.0	
80	21.7	20.5	19.5	18.5	17.5	17.3	E
75	21.4	20.0	19.0	18.0	17.0	16.5	
70	20.7	19.5	18.5	17.5	16.5	15.5	
65	19.8	19.0	18.0	17.0	16.0	15.0	
60	19.0	18.5	17.5	16.3	15.5	14.5	G
55	18.7	18.0	17.0	16.0	15.0	14.0	
50	18.0	17.5	16.5	15.3	14.5	13.5	
45	17.3	17.0	16.0	15.0	14.0	13.0	
40	16.5	16.5	15.5	14.3	13.3	12.5	F
35	16.0	16.0	15.0	14.0	12.5	12.0	
30	15.5	15.5	14.5	13.3	12.0	11.3	
25	14.1	15.0	13.8	12.5	11.2	10.5	
20	13.2	14.4	13.0	12.0	10.5	10.0	P
15	11.9	13.5	12.0	11.0	9.7	9.0	
10	10.5	12.3	11.0	10.0	8.5	8.0	
5	9.4	10.5	9.3	8.3	7.0	5.8	
1	<9.4	<10.5	<9.3	<8.3	<7.0	<5.8	VP
n	56	422	1,906	2,090	1,278	344	

Total n = 6,096

FLEXIBILITY – SIT AND REACH

Females

AGE

%	<20	20-29	30-39	40-49	50-59	60+	
99	>24.3	>24.5	>24.0	>22.8	>23.0	>23.0	
95	24.3	24.5	24.0	22.8	23.0	23.0	S
90	24.3	23.8	22.5	21.5	21.5	21.8	
85	22.5	23.0	22.0	21.3	21.0	19.5	
80	22.5	22.5	21.5	20.5	20.3	19.0	E
75	22.3	22.0	21.0	20.0	20.0	18.0	
70	22.0	21.5	20.5	19.8	19.3	17.5	
65	21.8	21.0	20.3	19.1	19.0	17.5	
60	21.5	20.5	20.0	19.0	18.5	17.0	G
55	21.3	20.3	19.5	18.5	18.0	17.0	
50	21.0	20.0	19.0	18.0	17.9	16.4	
45	20.5	19.5	18.5	18.0	17.0	16.1	
40	20.5	19.3	18.3	17.3	16.8	15.5	F
35	20.0	19.0	17.8	17.0	16.0	15.2	
30	19.5	18.3	17.3	16.5	15.5	14.4	
25	19.0	17.8	16.8	16.0	15.3	13.6	
20	18.5	17.0	16.5	15.0	14.8	13.0	P
15	17.8	16.4	15.5	14.0	14.0	11.5	
10	14.5	15.4	14.4	13.0	13.0	11.5	
5	14.5	14.1	12.0	10.5	12.3	9.2	
1	<14.5	<14.1	<12.0	<10.5	<12.3	<9.2	VP
n	19	183	376	332	192	44	

Total n = 1,146

DYNAMIC STRENGTH
1 Minute Sit Up

Males

AGE

%	<20	20-29	30-39	40-49	50-59	60+	
99	>62.0	>55.0	>51.0	>47.0	>43.0	>39.0	
95	62.0	55.0	51.0	47.0	43.0	39.0	S
90	55.0	52.0	48.0	43.0	39.0	35.0	
85	53.0	49.0	45.0	40.0	36.0	31.0	
80	51.0	47.0	43.0	39.0	35.0	30.0	E
75	50.0	46.0	42.0	37.0	33.0	28.0	
70	48.0	45.0	41.0	36.0	31.0	26.0	
65	48.0	44.0	40.0	35.0	30.0	24.0	
60	47.0	42.0	39.0	34.0	28.0	22.0	G
55	46.0	41.0	37.0	32.0	27.0	21.0	
50	45.0	40.0	36.0	31.0	26.0	20.0	
45	42.0	39.0	36.0	30.0	25.0	19.0	
40	41.0	38.0	35.0	29.0	24.0	19.0	F
35	39.0	37.0	33.0	28.0	22.0	18.0	
30	38.0	35.0	32.0	27.0	21.0	17.0	
25	37.0	35.0	31.0	26.0	20.0	16.0	
20	36.0	33.0	30.0	24.0	19.0	15.0	P
15	34.0	32.0	28.0	22.0	17.0	13.0	
10	33.0	30.0	26.0	22.0	15.0	10.0	
5	27.0	27.0	23.0	17.0	12.0	7.0	
1	<27.0	<27.0	<23.0	<17.0	<12.0	<7.0	VP
n	46	312	1,431	1,558	919	205	

Total n = 4,471

DYNAMIC STRENGTH
1 Minute Sit Up

Females

AGE

%	<20	20-29	30-39	40-49	50-59	60+	
99	>55.0	>51.0	>42.0	>38.0	>30.0	>28.0	
95	55.0	51.0	42.0	38.0	30.0	28.0	S
90	54.0	49.0	40.0	34.0	29.0	26.0	
85	49.0	45.0	38.0	32.0	25.0	20.0	
80	46.0	44.0	35.0	29.0	24.0	17.0	E
75	40.0	42.0	33.0	28.0	22.0	15.0	
70	38.0	41.0	32.0	27.0	22.0	12.0	
65	37.0	39.0	30.0	25.0	21.0	12.0	
60	36.0	38.0	29.0	24.0	20.0	11.0	G
55	35.0	37.0	28.0	23.0	19.0	10.0	
50	34.0	35.0	27.0	22.0	17.0	8.0	
45	34.0	34.0	26.0	21.0	16.0	8.0	
40	32.0	32.0	25.0	20.0	14.0	6.0	F
35	30.0	31.0	24.0	19.0	12.0	5.0	
30	29.0	30.0	22.0	17.0	12.0	4.0	
25	29.0	28.0	21.0	16.0	11.0	4.0	
20	28.0	24.0	20.0	14.0	10.0	3.0	P
15	27.0	23.0	18.0	13.0	7.0	2.0	
10	25.0	21.0	15.0	10.0	6.0	1.0	
5	25.0	18.0	11.0	7.0	5.0	0.0	
1	<25.0	<18.0	<11.0	<7.0	<5.0	0.0	VP
n	15	144	289	249	137	26	

Total n = 860

DYNAMIC STRENGTH
Push Up

Males

AGE

%	20-29	30-39	40-49	50-59	60+	
99	100	86	64	51	39	
95	62	52	40	39	28	S
90	57	46	36	30	26	
85	51	41	34	28	24	
80	47	39	30	25	23	E
75	44	36	29	24	22	
70	41	34	26	21	21	
65	39	31	25	20	20	
60	37	30	24	19	18	G
55	35	29	22	17	16	
50	33	27	21	15	15	
45	31	25	19	14	12	
40	29	24	18	13	10	F
35	27	21	16	11	9	
30	26	20	15	10	8	
25	24	19	13	9.5	7	
20	22	17	11	9	6	P
15	19	15	10	7	5	
10	18	13	9	6	4	
5	13	9	5	3	2	VP
n	1,045	790	364	172	26	

Total n = 2,397

DYNAMIC STRENGTH
Full Body Push Up*

Females

AGE

%	20-29	30-39	40-49	
99	53.0	48.0	23.0	
95	42.0	39.5	20.0	S
90	37.0	33.0	18.0	
85	33.0	26.0	17.0	
80	28.0	23.0	15.0	E
75	27.0	19.0	15.0	
70	24.0	18.0	14.0	
65	23.0	16.0	13.0	
60	21.0	15.0	13.0	G
55	19.0	14.0	11.0	
50	18.0	14.0	11.0	
45	17.0	13.0	10.0	
40	15.0	11.0	9.0	F
35	14.0	10.0	8.0	
30	13.0	9.0	7.0	
25	11.0	9.0	7.0	
20	10.0	8.0	6.0	P
15	9.0	6.5	5.0	
10	8.0	6.0	4.0	
5	6.0	4.0	1.0	
1	3.0	1.0	0.0	VP

* Full body push ups are generally used by law enforcement and public safety organizations.

Percent Fat Estimates For Women — Age to the Last Year

Sum of 3 Skinfolds	Age 22 and under	23 to 27	28 to 32	33 to 37	38 to 42	43 to 47	48 to 52	53 to 57	58 and over
23-25	9.7	9.9	10.2	10.4	10.7	10.9	11.2	11.4	11.7
26-28	11.0	11.2	11.5	11.7	12.0	12.3	12.5	12.7	13.0
29-31	12.3	12.5	12.8	13.0	13.3	13.5	13.8	14.0	14.3
32-34	13.6	13.8	14.0	14.3	14.5	14.8	15.0	15.3	15.5
35-37	14.8	15.0	15.3	15.5	15.8	16.0	16.3	16.5	16.8
38-40	16.0	16.3	16.5	16.7	17.0	17.2	17.5	17.7	18.0
41-43	17.2	17.4	17.7	17.9	18.2	18.4	18.7	18.9	19.2
44-46	18.3	18.6	18.8	19.1	19.3	19.6	19.8	20.1	20.3
47-49	19.5	19.7	20.0	20.2	20.5	20.7	21.0	21.2	21.5
50-52	20.6	20.8	21.1	21.3	21.6	21.8	22.1	22.3	22.6
53-55	21.7	21.9	22.1	22.4	22.6	22.9	23.1	23.4	23.6
56-58	22.7	23.0	23.2	23.4	23.7	23.9	24.2	24.4	24.7
59-61	23.7	24.0	24.2	24.5	24.7	25.0	25.2	25.5	25.7
62-64	24.7	25.0	25.2	25.5	25.7	26.0	26.2	26.4	26.7
65-67	25.7	25.9	26.2	26.4	26.7	26.9	27.2	27.4	27.7
68-70	26.6	26.9	27.1	27.4	27.6	27.9	28.1	28.4	28.6
71-73	27.5	27.8	28.0	28.3	28.5	28.8	29.0	29.3	29.5
74-76	28.4	28.7	28.9	29.2	29.4	29.7	29.9	30.2	30.4
77-79	29.3	29.5	29.8	30.0	30.3	30.5	30.8	31.0	31.3
80-82	30.1	30.4	30.6	30.9	31.1	31.4	31.6	31.9	32.1
83-85	30.9	31.2	31.4	31.7	31.9	32.2	32.4	32.7	32.9
86-88	31.7	32.0	32.2	32.5	32.7	32.9	33.2	33.4	33.7
89-91	32.5	32.7	33.0	33.2	33.5	33.7	33.9	34.2	34.4
92-94	33.2	33.4	33.7	33.9	34.2	34.4	34.7	34.9	35.2
95-97	33.9	34.1	34.4	34.6	34.9	35.1	35.4	35.6	35.9
98-100	34.6	34.8	35.1	35.3	35.5	35.8	36.0	36.3	36.5
101-103	35.2	35.4	35.7	35.9	36.2	36.4	36.7	36.9	37.2
104-106	35.8	36.1	36.3	36.6	36.8	37.1	37.3	37.5	37.8
107-109	36.4	36.7	36.9	37.1	37.4	37.6	37.9	38.1	38.4
110-112	37.0	37.2	37.5	37.7	38.0	38.2	38.5	38.7	38.9
113-115	37.5	37.8	38.0	38.2	38.5	38.7	39.0	39.2	39.5
116-118	38.0	38.3	38.5	38.8	39.0	39.3	39.5	39.7	40.0
119-121	38.5	38.7	39.0	39.2	39.5	39.7	40.0	40.2	40.5
122-124	39.0	39.2	39.4	39.7	39.9	40.2	40.4	40.7	40.9
125-127	39.4	39.6	39.9	40.1	40.4	40.6	40.9	41.1	41.4
128-130	39.8	40.0	40.3	40.5	40.8	41.0	41.1	41.5	41.8

Percent Fat Estimates For Men (40 & Under) — Age to the Last Year

Sum of 3 Skinfolds	Age 19 and under	20 to 22	23 to 25	26 to 28	29 to 31	32 to 34	35 to 37	38 to 40
11-13	1.9	2.3	2.6	3.0	3.3	3.7	4.0	4.3
14-16	2.9	3.3	3.6	3.9	4.3	4.6	5.0	5.3
17-19	3.9	4.2	4.6	4.9	5.3	5.6	6.0	6.3
20-22	4.8	5.2	5.5	5.9	6.2	6.6	6.7	7.3
23-25	5.8	6.2	6.5	6.8	7.2	7.5	7.9	8.2
26-28	6.8	7.1	7.5	7.8	8.1	8.5	8.8	9.2
29-31	7.7	8.0	8.4	8.7	9.1	9.4	9.8	10.1
32-34	8.6	9.0	9.3	9.7	10.0	10.4	10.7	11.1
35-37	9.5	9.9	10.2	10.6	10.9	11.3	11.6	12.0
38-40	10.5	10.8	11.2	11.5	11.8	12.2	12.5	12.9
41-43	11.4	11.7	12.1	12.4	12.7	13.1	13.4	13.8
44-46	12.2	12.6	12.9	13.3	13.6	14.0	14.3	14.7
47-49	13.1	13.5	13.8	14.2	14.5	14.9	15.2	15.5
50-52	14.0	14.3	14.7	15.0	15.4	15.7	16.1	16.4
53-55	14.8	15.2	15.5	15.9	16.2	16.6	16.9	17.3
56-58	15.7	16.0	16.4	16.7	17.1	17.4	17.8	18.1
59-61	16.5	16.9	17.2	17.6	17.9	18.3	18.6	19.0
62-64	17.4	17.7	18.1	18.4	18.8	19.1	19.4	19.8
65-67	18.2	18.5	18.9	19.2	19.6	19.9	20.3	20.6
68-70	19.0	19.3	19.7	20.0	20.4	20.7	21.1	21.4
71-73	19.8	20.1	20.5	20.8	21.2	21.5	21.9	22.2
74-76	20.6	20.9	21.3	21.6	22.0	22.3	22.7	23.0
77-79	21.4	21.7	22.1	22.4	22.8	23.1	23.4	23.8
80-82	22.1	22.5	22.8	23.2	23.5	23.9	24.2	24.6
83-85	22.9	23.2	23.6	23.9	24.3	24.6	25.0	25.3
86-88	23.6	24.0	24.3	24.7	25.0	25.4	25.7	26.1
89-91	24.4	24.7	25.1	25.4	25.8	26.1	26.5	26.8
92-94	25.1	25.5	25.8	26.2	26.5	26.9	27.2	27.5
95-97	25.8	26.2	26.5	26.9	27.2	27.6	27.9	28.3
98-100	26.6	26.9	27.3	27.6	27.9	28.3	28.6	29.0
101-103	27.3	27.6	28.0	28.3	28.6	29.0	29.3	29.7
104-106	27.9	28.3	28.6	29.0	29.3	29.7	30.0	30.4
107-109	28.6	29.0	29.3	29.7	30.0	30.4	30.7	31.1
110-112	29.3	29.6	30.0	30.3	30.7	31.0	31.4	31.7

Percent Fat Estimates For Men (Over 40) — Age to the Last Year

Sum of 3 Skinfolds	Age 41 to 43	44 to 46	47 to 49	50 to 52	53 to 55	56 to 58	59 to 61	62 and over
11-13	4.7	5.0	5.4	5.7	6.1	6.4	6.8	7.1
14-16	5.7	6.0	6.4	6.7	7.1	7.4	7.8	8.1
17-19	6.7	7.0	7.4	7.7	8.1	8.4	8.7	9.1
20-22	7.6	8.0	8.3	8.7	9.0	9.4	9.7	10.1
23-25	8.6	8.9	9.3	9.6	10.0	10.3	10.7	11.0
26-28	9.5	9.9	10.2	10.6	10.9	11.3	11.6	12.0
29-31	10.5	10.8	11.2	11.5	11.9	12.2	12.6	12.9
32-34	11.4	11.8	12.1	12.4	12.8	13.1	13.5	13.8
35-37	12.3	12.7	13.0	13.4	13.7	14.1	14.4	14.8
38-40	13.2	13.6	13.9	14.3	14.6	15.0	15.3	15.7
41-43	14.1	14.5	14.8	15.2	15.5	15.9	16.2	16.6
44-46	15.0	15.4	15.7	16.1	16.4	16.8	17.1	17.5
47-49	15.9	16.2	16.6	16.9	17.3	17.6	18.0	18.3
50-52	16.8	17.1	17.5	17.8	18.2	18.5	18.8	19.2
53-55	17.6	18.0	18.3	18.7	19.0	19.4	19.7	20.1
56-58	18.5	18.8	19.2	19.5	19.9	20.2	20.6	20.9
59-61	19.3	19.7	20.0	20.4	20.7	21.0	21.4	21.7
62-64	20.1	20.5	20.8	21.2	21.5	21.9	22.2	22.6
65-67	21.0	21.3	21.7	22.0	22.4	22.7	23.0	23.4
68-70	21.8	22.1	22.5	22.8	23.2	23.5	23.9	24.2
71-73	22.6	22.9	23.3	23.6	24.0	24.3	24.7	25.0
74-76	23.4	23.7	24.1	24.4	24.8	25.1	25.4	25.8
77-79	24.1	24.5	24.8	25.2	25.5	25.9	26.2	26.6
80-82	24.9	25.3	25.6	26.0	26.3	26.6	27.0	27.3
83-85	25.7	26.0	26.4	26.7	27.1	27.4	27.8	28.1
86-88	26.4	26.8	27.1	27.5	27.8	28.2	28.5	28.9
89-91	27.2	27.5	27.9	28.2	28.6	28.9	29.2	29.6
92-94	27.9	28.2	28.6	28.9	29.3	29.6	30.0	30.3
95-97	28.6	29.0	29.3	29.7	30.0	30.4	30.7	31.1
98-100	29.3	29.7	30.0	30.4	30.7	31.1	31.4	31.8
101-103	30.0	30.4	30.7	31.1	31.4	31.8	32.1	32.5
104-106	30.7	31.1	31.4	31.8	32.1	32.5	32.8	33.2
107-109	31.4	31.8	32.1	32.4	32.5	33.1	33.4	33.8
110-112	32.1	32.4	32.8	33.1	33.5	33.8	34.2	34.5

BODY COMPOSITION

Males

AGE

%	20-29	30-39	40-49	50-59	60-69	70-79	
99	4.2	7.0	9.2	10.9	11.5	13.6	
95	6.3	9.9	12.8	14.4	15.5	15.2	VL*
90	7.9	11.9	14.9	16.7	17.6	17.8	
85	9.2	13.3	16.3	18.0	18.8	19.2	
80	10.5	14.5	17.4	19.1	19.7	20.4	E
75	11.5	15.5	18.4	19.9	20.6	21.1	
70	12.7	16.5	19.1	20.7	21.3	21.6	
65	13.9	17.4	19.9	21.3	22.0	22.5	
60	14.8	18.2	20.6	22.1	22.6	23.1	G
55	15.8	19.0	21.3	22.7	23.2	23.7	
50	16.6	19.7	21.9	23.2	23.7	24.1	
45	17.4	20.4	22.6	23.9	24.4	24.4	
40	18.6	21.3	23.4	24.6	25.2	24.8	F
35	19.6	22.1	24.1	25.3	26.0	25.4	
30	20.6	23.0	24.8	26.0	26.7	26.0	
25	21.9	23.9	25.7	26.8	27.5	26.7	
20	23.1	24.9	26.6	27.8	28.4	27.6	P
15	24.6	26.2	27.7	28.9	29.4	28.9	
10	26.3	27.8	29.2	30.3	30.9	30.4	
5	28.9	30.2	31.2	32.5	32.9	32.4	
1	33.3	34.3	35.0	36.4	36.8	35.5	VP

n = 1826 8373 10442 6079 1836 301

Total n = 28,857

*Very Lean – No less than 3% body fat is recommended for males.

BODY COMPOSITION

Females

AGE

%	20-29	30-39	40-49	50-59	60-69	70-79	
99	9.8	11.0	12.6	14.6	13.9	14.6	
95	13.6	14.0	15.6	17.2	17.7	16.6	VL*
90	14.8	15.6	17.2	19.4	19.8	20.3	
85	15.8	16.6	18.6	20.9	21.4	23.0	
80	16.5	17.4	19.8	22.5	23.2	24.0	E
75	17.3	18.2	20.8	23.8	24.8	25.0	
70	18.0	19.1	21.9	25.1	25.9	26.2	
65	18.7	20.0	22.8	26.0	27.0	27.7	
60	19.4	20.8	23.8	27.0	27.9	28.6	G
55	20.1	21.7	24.8	27.9	28.7	29.7	
50	21.0	22.6	25.6	28.8	29.8	30.4	
45	21.9	23.5	26.5	29.7	30.6	31.3	
40	22.7	24.6	27.6	30.4	31.3	31.8	F
35	23.6	25.6	28.5	31.4	32.5	32.7	
30	24.5	26.7	29.6	32.5	33.3	33.9	
25	25.9	27.7	30.7	33.4	34.3	35.3	
20	27.1	29.1	31.9	34.5	35.4	36.0	P
15	28.9	30.9	33.5	35.6	36.2	37.4	
10	31.4	33.0	35.4	36.7	37.3	38.2	
5	35.2	35.8	37.4	38.3	39.0	39.3	
1	38.9	39.4	39.8	40.4	40.8	40.5	VP

n = 1360 3597 3808 2366 849 136

Total n = 12,116

*Very Lean - No less than 10-13% body fat is recommended for females.

ATTACHMENT I

HEALTH AND WELLNESS ASSESSMENT CHECKLIST

1. Review of PRT test scores (provide trend analysis from database)
2. Recommendations for improvement (upon request by special agent)
 - Fitness plan for flexibility
 - Fitness plan for cardiovascular
 - Fitness plan for strength
3. Nutrition/dietary review (see supplemental material and DCIS Handbook)
4. Optional Blood Pressure Reading
5. Optional Weight/Body composition analysis (BMI, skin caliper measurement)
6. Stress management techniques
7. Review of Supplemental Materials
8. Does the criminal investigator have a copy of the DCIS Health and Wellness Handbook?
9. Program feedback



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

June 30, 2016

MEMORANDUM FOR ALL DCIS SPECIAL AGENTS

SUBJECT: Interim Policy for Special Agents Manual (SAM) Chapter 58, "Health and Wellness Program," regarding a Decrease in the Frequency of Physical Readiness Assessments

Effective immediately, this interim policy modifies guidance provided in SAM Chapter 58 to reduce the frequency of the Physical Readiness Assessment (PRA) formerly known as the Physical Readiness Test (PRT) from semiannually to once per year.

SAM Chapter 58, paragraph 58.6.a. currently states, in part:

The PRT will be administered semiannually (spring and fall) in one continuous session. All special agents who have been medically cleared by the FOH MRO are required to participate in the PRT as a duty associated with their position as criminal investigators...

This citation is amended to read as follows:

The PRA will be administered once annually in one continuous session before the end of the fiscal year (September 30). The timing of the PRA will be at the discretion of the cognizant field office or headquarters Health and Wellness Coordinator, with due consideration given to seasonal weather conditions. All special agents are required to participate in the PRA as a duty associated with their position as criminal investigators...

Additionally, all other references in SAM Chapter 58 to a semiannual PRA are effectively changed to align with the above amendment.

This policy is in effect until it is rescinded or incorporated into the next revision of SAM Chapter 58. Any questions related to this policy should be directed to me at (703) 604-6, (b)(7)

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

Deputy Assistant Inspector General
for Investigations



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
4800 MARK CENTER DRIVE
ALEXANDRIA, VIRGINIA 22350-1500

June 30, 2016

MEMORANDUM FOR ALL DCIS SPECIAL AGENTS

SUBJECT: Interim Policy for Special Agents Manual (SAM) Chapter 58, "Health and Wellness Program," regarding an Increase in Authorized Physical Training Hours

Effective immediately, this interim policy modifies guidance provided in SAM Chapter 58 to increase the number of authorized on-duty physical training (PT) hours from 4 hours to 5 hours per week.

SAM Chapter 58, paragraph 58.10.a. currently states:

Special agents are encouraged to participate in PT. To this end, 4 hours of official on-duty time per week are authorized, provided that the criminal investigator participates in the PRT and the duty schedule otherwise permits it. Special agents using 4 hours of official on-duty time per week for PT cannot also use physical fitness time under OIG Instruction 6100.2, "Physical Fitness Program."

This citation is amended to read as follows:

Special agents are encouraged to participate in PT. To this end, 5 hours of official on-duty time per week are authorized, provided that the criminal investigator participates in the PRA and the duty schedule otherwise permits it.

Furthermore, all other references in SAM Chapter 58 to 4 hours of PT time are effectively changed to align with the above amendment.

This policy is in effect until it is rescinded or incorporated into the next revision of SAM Chapter 58. Any questions related to this policy should be directed to me at (703) 604-(b)(6), (b)(7)

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

Deputy Assistant Inspector General
for Investigations

CHAPTER 59

VOLUNTARY TRANSFER PROGRAM

<u>Contents</u>	<u>Section</u>
General	59.1.
Approval	59.2.
VTP Procedures	59.3.
VTP Eligibility Requirements	59.4.

59.1. General. The Defense Criminal Investigative Service (DCIS) Voluntary Transfer Program (VTP) is designed to provide DCIS Special Agents an opportunity to change duty locations to an office of personal preference where an opening exists. The VTP will be approved on a case-by-case basis.

59.2. Approval. Approval of the VTP rests with the Deputy Inspector General-Investigations (DIG-INV).

59.3. VTP Procedures

59.3.a. DCIS identifies an opening in a specific duty location.

59.3.b. The field office Special Agent in Charge (SAC) elects and requests to fill that opening via the VTP.

59.3.c. After approval by the DIG-INV, the Internal Operations Directorate will issue an e-mail notification of the opening, giving interested candidates 10 days to submit their name for consideration.

59.3.d. The SAC of the gaining field office may select from those who apply and meet the eligibility requirements (see section 59.4). The gaining SAC may choose not to select any of the applicants. The gaining office, in coordination with the applicant's current field office, will notify those persons not selected.

59.3.e. The "gaining" SAC, the "losing" SAC, and the selected employee will establish a reporting date, which typically will be within 90 days following notification of the selection. If beyond 90 days, approval must be obtained from the gaining SAC.

59.3.f. In the event there are no VTP applicants, no applicants meet the eligibility requirements, or the gaining SAC selects no VTP applicant, normal hiring procedures will be used.

59.4. VTP Eligibility Requirements

59.4.a. The employee must sign an agreement to move at personal expense. Generally, Permanent Change of Station (PCS) funds will not be paid. Additionally, administrative leave will not be approved for non-PCS voluntary transfers.

59.4.b. The employee must have been employed by DCIS for at least 36 months. In the event there are no VTP applicants that meet this time-with-Agency criteria, the cognizant field office SAC may request approval to waive this requirement through the DIG-INV.

59.4.c. The employee's last two performance appraisal must have been "Fully Successful" or better.

59.4.d. The employee's current SAC must recommend the employee.