



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

Released date: 22-March-2017

Posted date: 27-March-2017

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		d. COMPUTATIONS	
16. 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		18. POC TRAVEL (X one) <input type="checkbox"/> OWN/OPERATE <input type="checkbox"/> PASSENGER		17. DURATION OF TRAVEL <input type="checkbox"/> 12 HOURS OR LESS <input type="checkbox"/> MORE THAN 12 HOURS BUT 24 HOURS OR LESS <input type="checkbox"/> MORE THAN 24 HOURS		19. GOVERNMENT DEDUCTIBLE MEALS a. DATE b. NO. OF MEALS c. DATE d. NO. OF MEALS	
20. CLAIMANT SIGNATURE		21. REVIEWER'S PRINTED NAME		22. REVIEWER SIGNATURE		23. TELEPHONE NUMBER	
24. APPROVING OFFICIAL'S PRINTED NAME		25. SIGNATURE		26. TELEPHONE NUMBER		27. DATE	
28. ACCOUNTING CLASSIFICATION							
29. COLLECTION DATA							
30. COMPUTED BY		31. AUDITED BY		32. TRAVEL ORDER AUTHORIZATION POSTED BY		33. RECEIVED (Payee Signature and Date or Check No.)	
34. AMOUNT PAID							

DD FORM 1351-2, MAR 2008

PREVIOUS EDITION MAY BE USED UNTIL SUPPLY IS EXHAUSTED.

Exception to SF 1012 approved by GSA/IRMS 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

PREVIOUS EDITION MAY BE USED UNTIL SUPPLY IS EXHAUSTED.

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

**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

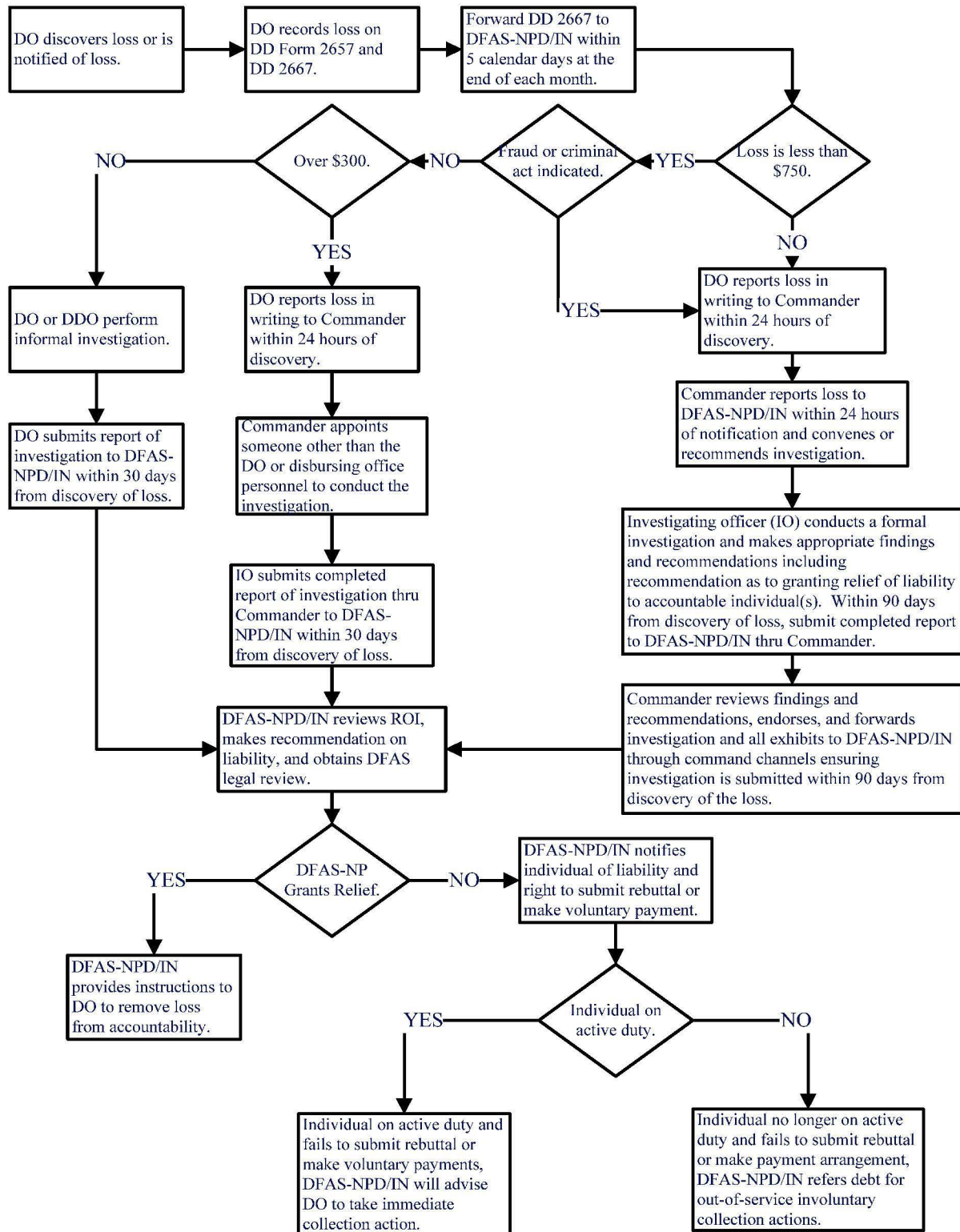


Table 6-2. Processing Physical Losses of Funds

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,		<p>Upon discovery, report loss to DO or authorized agent who advanced the funds through the commander who approved establishment of funds, and</p> <p>Make a return (on paper only) of the amount of the loss using the DD Form 1081.</p> <p>Upon receipt of additional advance, if applicable, provide the DO with a signed DD Form 1081.</p>	<p>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> <p>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.</p>	<p>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.</p> <p>2. If loss is a minor loss of funds, ensure investigation is conducted per paragraph 060105.B of this chapter.</p> <p>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.</p> <p>a. Include information as to whether imprest fund will be turned over to alternate cashier pending completion of the required investigation(s) and</p> <p>b. Provide instructions of the additional advance to the primary or alternate cashier, as appropriate.</p>

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

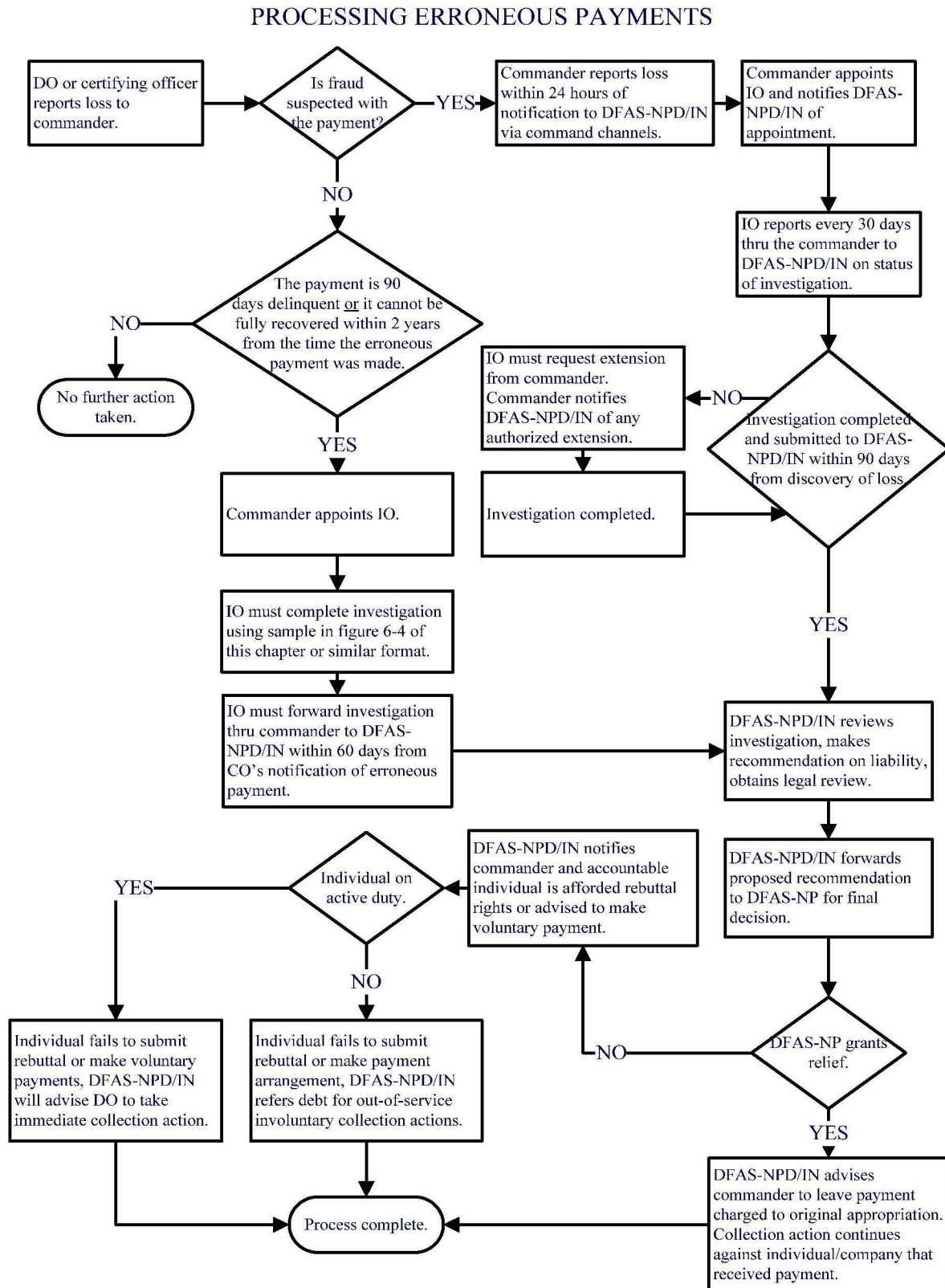
Question	Cashier Loss	Counterfeit Currency Loss	Agent Officer Loss	Fraud Loss	Imprest Fund Cashier and Change Fund Custodian Loss
Has the DO issued any oral instructions?	X	X	X		
Was the cashier's cage or safe accessible to persons other than the cashier/agent?	X		X		
Did theft occur?	X		X		X
Does the 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 RFPAs 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 RFPAs.

14.14.b. Because the RFPAs contemplate that law enforcement authorities must proceed under the RFPAs 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 RFPAs set 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